



FARONICS
ANTI-VIRUS™

Protección CONFIABLE de las amenazas

Guía del usuario



FARONICS™
Intelligent Solutions for ABSOLUTE Control

www.faronics.com



Modificado por última vez: setiembre de 2015

© 1999 - 2015 Faronics Corporation. Todos los derechos reservados. Faronics, Deep Freeze, Faronics Core Console, Faronics Anti-Executable, Faronics Anti-Virus, Faronics Device Filter, Faronics Data Igloo, Faronics Power Save, Faronics Insight, Faronics System Profiler y WINSelect son marcas comerciales o marcas registradas de Faronics Corporation. El resto de los nombres de productos y compañías son marcas comerciales de sus respectivos dueños.



Contenidos

Prólogo	5
Información importante	6
Acerca de Faronics	6
Documentación del producto	6
Soporte Técnico	7
Información de contacto	7
Definición de términos	8
Introducción	11
Generalidades sobre Faronics Anti-Virus	12
Requisitos del sistema	13
Requisitos de Faronics Anti-Virus	13
Requisitos de Faronics Core	13
Requisitos de Deep Freeze	13
Licencia de Faronics Anti-Virus	14
Instalación de Faronics Anti-Virus	15
Descripción general de la instalación	16
Instalación de Faronics Core	16
Instalación de Faronics Anti-Virus Loadin	17
Instalación o actualización de Faronics Anti-Virus en una estación de trabajo mediante Faronics Core Console	20
Instalación manual de Faronics Anti-Virus en una estación de trabajo	21
Uso de Faronics Anti-Virus	25
Generalidades sobre Faronics Anti-Virus	26
Administración de Faronics Anti-Virus a través de Faronics Core Console	27
Implementación de Faronics Anti-Virus Client en las estaciones de trabajo	27
Configuración de Faronics Anti-Virus	27
Actualización de la configuración de Faronics Anti-Virus	29
Política de Faronics Anti-Virus	30
Creación de políticas Anti-Virus	30
Aplicación de una política Anti-Virus	56
Visualización o modificación de una política Anti-Virus	57
Renombrar una política Anti-Virus	57
Copiar una política	57
Eliminar una política Anti-Virus	58
Importar una política Anti-Virus	58
Exportar una política Anti-Virus	58
Análisis mediante Faronics Core Console	60
Ver y tomar medidas acerca de los archivos en cuarentena	61
Cómo ver los registros de Faronics Anti-Virus	63
Actualización de Faronics Anti-Virus a través de Faronics Core Console	67
Programación de acciones para Faronics Anti-Virus a través de Faronics Core Console	68



Generación de informes	69
Informes globales	69
Informes específicos de una estación de trabajo	69
Uso de Faronics Anti-Virus en la estación de trabajo	71
Inicio de Faronics Anti-Virus en la estación de trabajo	71
Análisis de la estación de trabajo	72
Análisis de un archivo o una carpeta con clic del botón derecho	74
Ver historial de análisis	74
Ver y tomar medidas acerca de los archivos en cuarentena	75
Actualización de las definiciones anti-virus en la estación de trabajo	77
Administración de Faronics Anti-Virus en la estación de trabajo a través de la bandeja de sistema	78
Control de línea de comandos	79
Control de línea de comandos	80
Desinstalación de Faronics Anti-Virus	81
Generalidades sobre la desinstalación	82
Desinstalación de Faronics Anti-Virus Client a través de Faronics Core Console	83
Desinstalación de Faronics Anti-Virus Client de una estación de trabajo a través de Add or Remove Programs (Agregar o quitar programas)	84
Desinstalación de Faronics Anti-Virus Loadin con el instalador	85
Desinstalación de Faronics Anti-Virus a través de Agregar o Quitar Programas	87



Prólogo

Esta guía del usuario explica cómo instalar y usar Faronics Anti-Virus.

Temas

Información importante

Soporte Técnico

Definición de términos



Información importante

Esta sección contiene información importante acerca de su producto de Faronics.

Acerca de Faronics

Faronics brinda soluciones líderes en el mercado que ayudan a administrar, simplificar y proteger entornos complejos de TI. Nuestros productos garantizan una disponibilidad del 100% para las máquinas y han repercutido notablemente en la vida cotidiana de miles de profesionales de tecnología de la información. Impulsadas por su orientación al mercado, las innovaciones tecnológicas de Faronics benefician a instituciones educativas, centros de salud, bibliotecas, organizaciones gubernamentales y empresas.

Documentación del producto

Los siguientes documentos integran el conjunto de documentación de Faronics Anti-Virus:

- Guía del usuario *Faronics Anti-Virus*: Este documento le indicará cómo usar el producto.
- Notas de la versión de *Faronics Anti-Virus*: Este documento enumera las nuevas funciones, los temas conocidos y los temas cerrados.



Soporte Técnico

Hemos puesto todo nuestro esfuerzo para diseñar un software de fácil utilización y que no presente inconvenientes. De presentarse alguno, póngase en contacto con nuestro Soporte Técnico.

Correo electrónico: support@faronics.com

Teléfono: 1-800-943-6422 ó 1-604-637-3333

Horario: De lunes a viernes, de 7:00 a.m. a 5:00 p.m. (Hora del Pacífico)

Información de contacto

- Web: www.faronics.com
- Correo electrónico: sales@faronics.com
- Teléfono: 1-800-943-6422 ó 1-604-637-3333
- Fax: 1-800-943-6488 ó 1-604-637-8188
- Horario: De lunes a viernes, de 7:00 a.m. a 5:00 p.m. (Hora del Pacífico)
- Dirección: Faronics Technologies USA Inc.
2411 Old Crow Canyon Road, Suite 170
San Ramón, CA 94583
EE.UU.

Faronics Corporation (Canadá e internacional)
609 Granville Street, Suite 1400
Vancouver, BC V7Y 1G5
Canadá

Faronics Corporation (Europa)
Siena Court
The Broadway Maidenhead
Berkshire, SL6 1NJ UK



Definición de términos

Término	Definición
Protección activa	La protección activa (Active Protection, AP) es un método de detección de malware en tiempo real. AP trabaja en segundo plano mientras usted trabaja o navega por Internet, monitoreando constantemente los archivos que se ejecutan sin causar un esfuerzo notorio en su sistema.
Adware	El adware, también conocido como software de publicidad, por lo general se basa en el contexto o el comportamiento y registra los hábitos de navegación para mostrar publicidades de terceros cuyo destino es el usuario relevante. Las publicidades pueden tener diferentes formas, entre ellas ventanas emergentes, ventanas inferiores, pancartas o enlaces que contienen páginas Web o partes de la interfaz de Windows. Algunas publicidades de adware pueden consistir en publicidades de texto que se muestran dentro de la misma aplicación o dentro de las barras laterales, las barras de búsqueda y los resultados de las búsquedas.
Protección del correo electrónico	La protección del correo electrónico es una herramienta detrás de escena que protege a su computadora de los mensajes de correo electrónico entrantes y salientes que puedan ser dañinos. Siempre y cuando tenga habilitada la protección del correo electrónico, su computadora está protegida con análisis automático de todos los adjuntos en busca de malware y virus sin que tenga que hacer nada.
Cuarentena	La cuarentena es un lugar seguro de su computadora usa Faronics Anti-Virus para almacenar el malware o los archivos infectados que no se pudieron desinfectar. Si su computadora o los archivos de su computadora no están actuando normalmente luego de haber colocado el elemento ahí, usted tiene la oportunidad de revisar los detalles de un riesgo e investigarlo más y quitarlo de la Cuarentena, restaurarlo a la computadora en su ubicación original. También puede retirar permanentemente los riesgos de la Cuarentena.
Firewall	Un Firewall proporciona protección bidireccional que lo protege del tránsito entrante y saliente. Un Firewall protege su red de intrusos no autorizados.



Término	Definición
Programa de seguridad de uso deshonesto	Un programa de uso deshonesto es un software de origen desconocido o cuestionable, o de valor dudoso. Un programa de seguridad de uso deshonesto por lo general aparece en sitios Web o mensajes de correo electrónico con spam como advertencias intrusivas que dicen que su computadora está infectada y ofrecen analizarla y limpiarla. Nunca se debe confiar en este tipo de mensajes. Las compañías antivirus o antispyware nunca usaran esta forma de <i>notificación</i> . Un programa de seguridad de uso deshonesto puede tener la apariencia de un antivirus común o de un programa antimalware, pero en vez de eso intenta engañarlo para que compre el programa. Mientras que algunos programas de seguridad deshonestos son el equivalente al <i>vendedor de cosas inútiles</i> que engaña a los clientes, otros pueden resultar dañinos ya que instalan malware o incluso roban la información crediticia que usted ingresa y posiblemente realizan robo de identidad. Además, usted tiene que ser cuidadoso al cerrar o eliminar estas alertas, incluso cuando sabe que son falsas.
Rootkits	Un software rootkit oculta la presencia de los archivos y los datos para evadir la detección, mientras permite que un atacante controle la máquina sin que el usuario lo sepa. Por lo general, los rootkits son utilizados por los virus, spyware, troyanos y programas encubiertos, para ocultarse del usuario y del software de detección de malware como las aplicaciones anti-virus y anti-spyware. Los rootkits también son utilizados por algunas aplicaciones de adware y DRM (Digital Rights Management, administración de derechos digitales) para evitar que los usuarios eliminen ese software no deseado.
Spyware	El spyware es un software que transmite información a un tercero sin notificárselo a usted. También se lo conoce como trackware, hijackware, scumware, snoopware y thiefware. Algunos defensores de la privacidad incluso lo llaman control de acceso legítimo, filtrado, monitoreo de Internet, recuperación de contraseña, seguridad y software de supervisión <i>spyware</i> porque estos se pueden usar sin notificarle a usted.
Troyano	Un troyano se instala en forma fraudulenta o con falsedades y con frecuencia sin que el usuario lo conozca del todo o dé su consentimiento. En otras palabras, lo que puede parecer completamente inofensivo para un usuario, de hecho es dañino porque contiene código malicioso. La mayoría de los troyanos tienen alguna forma de funcionalidad o comportamiento malicioso, hostil o dañino.
Virus	Un virus de computación es un código malicioso que tiene la capacidad de replicarse a sí mismo e invadir otros programas o archivos para extenderse en la máquina infectada. Típicamente, los virus se expanden cuando los usuarios ejecutan los archivos infectados o cargan medios infectados, en especial medios extraíbles como CD-ROM o unidades flash. Los virus también se pueden expandir a través del correo electrónico con adjuntos y archivos infectados. La mayoría de los virus incluyen una <i>carga</i> que puede estar en cualquier parte desde molesto o que interrumpe hasta dañino. Los virus pueden causar daños en el sistema, pérdidas de datos valiosos o se pueden utilizar para instalar otro malware.



Término	Definición
Gusano	Un gusano es un programa malicioso que se expande sin la intervención de ningún usuario. Los gusanos son similares a los virus porque se auto-repican. Sin embargo, a diferencia de los virus, los gusanos se expanden sin adjuntarse o infectar otros programas y archivos. Un gusano se puede expandir por las redes de computación a través de agujeros de seguridad en las máquinas vulnerables conectadas a la red. Los gusanos también pueden expandirse a través del correo electrónico mediante el envío de copias de sí mismo a todos los contactos de la libreta de direcciones. Un gusano puede consumir una gran cantidad de recursos del sistema y hacer que la máquina se vuelva notablemente más lenta y poco confiable. Algunos gusanos se pueden usar para comprometer a las máquinas infectadas y descargar software malicioso adicional.



Introducción

Faronics Anti-Virus proporciona protección de las amenazas de seguridad sin hacer que las computadoras funcionen con lentitud debido a los tiempos de análisis lentos y espacios de utilización grandes. Construido con tecnología de última generación, Faronics Anti-Virus le proporciona un software anti-virus y anti-spyware poderoso todo en uno que lo protege de las amenazas complejas de malware actuales, mientras que a la vez proporciona una integración perfecta con *Faronics Deep Freeze* y *Faronics Anti-Executable* para así conformar una solución de seguridad muy completa en varios niveles.

Temas

[Generalidades sobre Faronics Anti-Virus](#)

[Requisitos del sistema](#)

[Licencia de Faronics Anti-Virus](#)



Generalidades sobre Faronics Anti-Virus

Faronics Anti-Virus protege a las estaciones de trabajo de las siguientes amenazas:

- Adware
- Programa de seguridad de uso deshonesto
- Rootkits
- Spyware
- Troyano
- Gusanos

Faronics Anti-Virus se puede implementar en múltiples estaciones de trabajo a través de Faronics Core. Para obtener información sobre Faronics Core, consulte la Guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en <http://www.faronics.com/library>.

Cuando se instala con Deep Freeze, las definiciones Anti-Virus se pueden actualizar en las estaciones de trabajo administradas sin que sea necesario *Reiniciar Thawed* o reiniciar en *Modo mantenimiento*. Para obtener más información consulte la Guía del usuario de Deep Freeze Enterprise. La guía del usuario más reciente está disponible en <http://www.faronics.com/library>.



Requisitos del sistema

Requisitos de Faronics Anti-Virus

El Loadin de Faronics Anti-Virus tiene los siguientes requisitos:

- Faronics Core 3.7 o superior

El cliente Faronics Anti-Virus en la estación de trabajo requiere cualquiera de los siguientes sistemas operativos:

- Windows XP SP3 (32 bits) o Windows XP SP2 (64 bits)
- Windows Vista SP2 (32 bits o 64 bits)
- Windows 7 (32 bits o 64 bits)
- Windows 8.1 (32 bits o 64 bits)
- Windows 10 (32 bits o 64 bits)
- Windows Server 2003 (32 bits o 64 bits)
- Windows Server 2008 R2 (64 bits)
- Windows Server 2012 (64 bits)

Se recomienda instalar todos los componentes usando una cuenta de Administrador de Windows.

Requisitos de Faronics Core

Es posible encontrar información sobre los requisitos del sistema en la Guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en <http://www.faronics.com/library>.

Requisitos de Deep Freeze

Es posible encontrar información sobre los requisitos del sistema de Deep Freeze en la Guía del usuario de Deep Freeze Enterprise. La guía del usuario más reciente está disponible en <http://www.faronics.com/library>.



Para ejecutar Faronics Anti-Virus en las estaciones de trabajo administradas por Deep Freeze, se necesita Deep Freeze Enterprise 7.0 o superior.



Licencia de Faronics Anti-Virus

La licencia de Faronics Anti-Virus se puede aplicar a través de Faronics Core Console. Realice los siguientes pasos para aplicar la Licencia de Faronics Anti-Virus:

1. Inicie Faronics Core Console.
2. Haga clic con el botón derecho del mouse en *Core Server* y elija *Properties (Propiedades)*.
3. Haga clic en la ficha *Anti-virus*. La ficha Anti-Virus muestra la *Versión*, *Clave de licencia* (si es una versión con licencia), y *Vencimiento de la licencia*.
4. Haga clic en *Editar* e ingrese la *clave de licencia* en el campo *Clave de licencia*.
5. Haga clic en *Apply (Aplicar)*. Haga clic en *OK (Aceptar)*.



Si la clave de licencia de Faronics Anti-Virus se ingresó cuando se instaló el Loadin, no es necesario ingresarla nuevamente en la ficha *Propiedades*.



Las definiciones de virus no se pueden descargar si la licencia de Faronics Anti-Virus está vencida.

Las licencias de Faronics Anti-Virus funcionan de la siguiente forma:

- Core Server (un componente de Faronics Core) envía automáticamente la clave de licencia a las estaciones de trabajo en las que está instalado Faronics Anti-Virus Client (si las computadoras están desconectadas, la clave de licencia se aplicará una vez que las computadoras estén nuevamente en línea).
- La clave de licencia no se puede editar manualmente en la estación de trabajo.



Instalación de Faronics Anti-Virus

Este capítulo describe cómo instalar Faronics Anti-Virus.

Temas

Descripción general de la instalación

Instalación de Faronics Anti-Virus Loadin

Instalación o actualización de Faronics Anti-Virus en una estación de trabajo mediante Faronics Core Console

Instalación manual de Faronics Anti-Virus en una estación de trabajo



Descripción general de la instalación

Faronics Anti-Virus tiene dos componentes:

- Faronics Anti-Virus Loadin: se instala en una computadora que tiene Faronics Core.
- Cliente Faronics Anti-Virus: se implementa en una estación de trabajo que será administrada por Faronics Anti-Virus Loadin.

La instalación y configuración de la consola Faronics Anti-Virus implica las siguientes etapas:

- Instalar Faronics Core y generar/implementar Core Agent
- Instalación de Faronics Anti-Virus Loadin
- Implementación del Cliente Faronics Anti-Virus

Instalación de Faronics Core

Para obtener información sobre cómo instalar la Faronics Core y generar/implementar el instalador de Core Agent, consulte la guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en <http://www.faronics.com/library>.



Instalación de Faronics Anti-Virus Loadin

Realice los siguientes pasos para instalar Faronics Anti-Virus Loadin:



No es posible instalar Anti-Virus Loadin en un equipo que no tenga también instalado Faronics Core Console (o Faronics Core Server).

1. Haga doble clic en *Anti-VirusLoadinInstaller.exe*. Haga clic en *Next (Siguiente)*.



2. Lea y acepte el contrato de licencia. Haga clic en *Next (Siguiente)*.

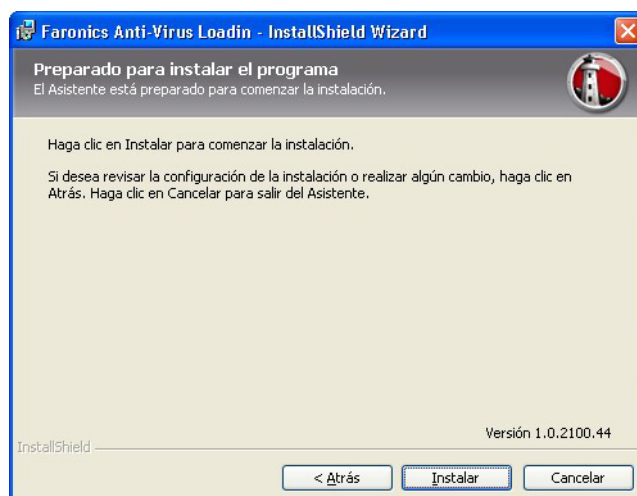




3. Ingrese el *Nombre de usuario*, la *Organización* y la *Clave de licencia*. Alternativamente, seleccione la casilla de verificación *Use Evaluation (Usar evaluación)*. Faronics Anti-Virus caduca luego de 30 días de evaluación. Haga clic en *Next (Siguiente)*.

4. La ubicación predeterminada es *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus*.

5. Haga clic en *Install (Instalar)* para instalar Faronics Anti-Virus Loadin.



6. Se mostrará el siguiente mensaje. Haga clic en *Yes (Sí)* para reiniciar el servicio Faronics Core Server. Haga clic en *No* para reiniciar manualmente el servicio Faronics Core Server.



7. Haga clic en *Finish (Finalizar)* para completar la instalación.





Instalación o actualización de Faronics Anti-Virus en una estación de trabajo mediante Faronics Core Console

Core Agent, que forma parte de Faronics Core, debe ser instalado en cada estación de trabajo que será administrada por Faronics Anti-Virus. Para más información sobre la instalación de Core Agent, consulte la guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en <http://www.faronics.com/library>.

Las estaciones de trabajo se detectan en la red después de la instalación de Core Agent y pueden verse en Core Console.

Para instalar o actualizar la versión de Faronics Anti-Virus, seleccione una o varias estaciones de trabajo:

1. Haga clic en Configurar estaciones de trabajo en el panel derecho y seleccione *Avanzado > Instalar/Actualizar la versión de Faronics Anti-Virus Client*.
2. Seleccione las siguientes opciones si tiene instalado otro programa antivirus:
 - Quite cualquier producto antivirus no compatible antes de instalar Faronics Anti-Virus Enterprise Workstation.
 - Instalar Faronics Anti-Virus incluso si hay otro producto Anti-Virus o si no se pudo quitar.



La estación de trabajo se reinicia después de una instalación o una actualización exitosa.



Si hay más de un Loadin instalado, se puede acceder al menú contextual de Faronics Anti-Virus al hacer clic derecho en una estación de trabajo, seleccionar *Anti-Virus* y luego seleccionar la acción en particular.



Instalación manual de Faronics Anti-Virus en una estación de trabajo

Antes de instalar Faronics Anti-Virus Client en una estación de trabajo, copie el archivo *msi* apropiado desde la ruta *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus\Wks Installers* en el equipo donde está instalado Anti-Virus Loadin en una o más estaciones de trabajo.

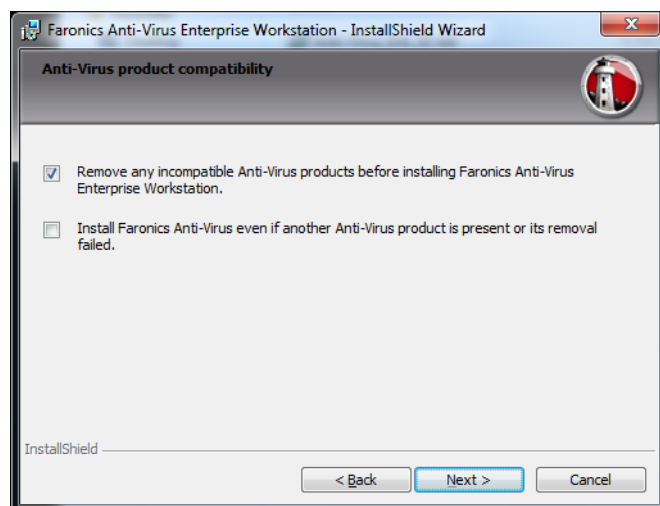
Repita el proceso en cada estación de trabajo que se protegerá con Faronics Anti-Virus.

Realice los siguientes pasos para instalar Faronics Anti-Virus en la estación de trabajo:

1. Haga doble clic en *AntiVirus_Ent_32-bit.msi* en un sistema operativo de 32 bits y en *AntiVirus_Ent_64-bit.msi* en un sistema operativo de 64 bits. Haga clic en *Next (Siguiente)*.



2. Seleccione las siguientes opciones si tiene instalado otro programa antivirus:
 - Quite cualquier producto antivirus no compatible antes de instalar Faronics Anti-Virus Enterprise Workstation.
 - Instalar Faronics Anti-Virus incluso si hay otro producto Anti-Virus o si no se pudo quitar.

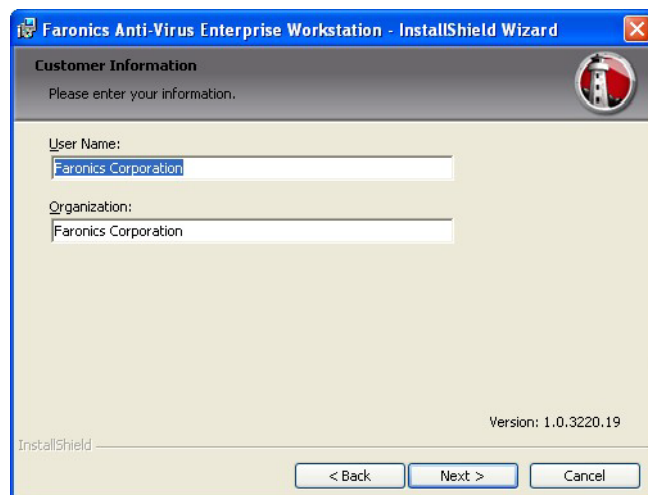




3. Lea y acepte el contrato de licencia. Haga clic en *Next (Siguiente)*.



4. Ingrese el *Nombre de usuario* y la *Organización*. Haga clic en *Next (Siguiente)*.

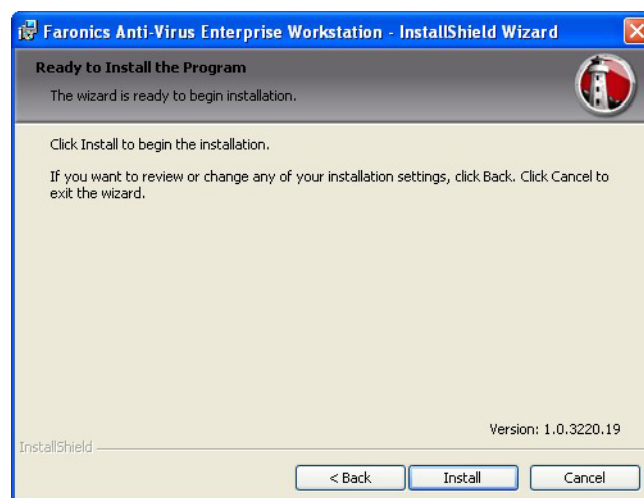




5. La ubicación predeterminada es *C:\Program Files\Faronics\Faronics Anti-Virus Enterprise*. Haga clic en *Change...* (*Cambiar...*) para cambiar la ubicación en la que se instalará Faronics Anti-Virus. Haga clic en *Next* (*Siguiente*).



6. Haga clic en *Install* (*Instalar*) para instalar Faronics Anti-Virus.



7. Haga clic en *Finish* (*Finalizar*) para completar la instalación.





Se recomienda reiniciar de inmediato luego de instalar el cliente Anti-Virus en la estación de trabajo.



Uso de Faronics Anti-Virus

Este capítulo describe cómo usar Faronics Anti-Virus.

Temas

Generalidades sobre Faronics Anti-Virus

Administración de Faronics Anti-Virus a través de Faronics Core Console

Política de Faronics Anti-Virus

Análisis mediante Faronics Core Console

Ver y tomar medidas acerca de los archivos en cuarentena

Cómo ver los registros de Faronics Anti-Virus

Actualización de Faronics Anti-Virus a través de Faronics Core Console

Generación de informes

Uso de Faronics Anti-Virus en la estación de trabajo

Administración de Faronics Anti-Virus en la estación de trabajo a través de la bandeja de sistema



Generalidades sobre Faronics Anti-Virus

Faronics Anti-Virus se puede usar de las siguientes formas:

Administración de Faronics Anti-Virus a través de Faronics Core Console:

- Instalación de Faronics Anti-Virus Loadin (para más información, consulte [Instalación de Faronics Anti-Virus Loadin](#))
- Implementar Faronics Anti-Virus Client en las estaciones de trabajo
- Crear, editar, eliminar y aplicar una política anti-virus
- Analizar las estaciones de trabajo a través de Faronics Core Console
- Ver y tomar medidas acerca de los archivos en cuarentena
- Actualizar las definiciones anti-virus a través de Faronics Core Console
- Generación de informes

Uso de Faronics Anti-Virus en la estación de trabajo

- Inicio de Faronics Anti-Virus en la estación de trabajo
- Análisis de la estación de trabajo
- Actualización de las definiciones anti-virus en la estación de trabajo.



Administración de Faronics Anti-Virus a través de Faronics Core Console

Una vez instalado Faronics Anti-Virus Loadin, las estaciones de trabajo se pueden administrar a través de Faronics Core Console. En las siguientes secciones se explican varios aspectos de la administración de Faronics Anti-Virus a través de Faronics Core Console.

Implementación de Faronics Anti-Virus Client en las estaciones de trabajo

Realice los siguientes pasos para implementar Faronics Anti-Virus Client en las estaciones de trabajo:

1. Inicie Faronics Core Console.
2. En el panel Console Tree (Árbol de la consola), vaya a *Faronics Core Console*>[Nombre de Core Server]>Workstations (Estaciones de trabajo)>Managed Workstations (Estaciones de trabajo administradas).
3. Haga clic con el botón derecho en una o más estaciones de trabajo y seleccione *Configure Workstations (Configurar estaciones de trabajo)*>*Advanced (Avanzado)*>*Install/Upgrade Anti-Virus Client (Instalar/Actualizar Anti-Virus Client)*.

Faronics Anti-Virus está instalado en las estaciones de trabajo.



Luego de una implementación satisfactoria, la estación de trabajo tendrá la política Default (Predeterminada) y las últimas definiciones de virus.

Configuración de Faronics Anti-Virus

Realice los siguientes pasos para configurar Faronics Anti-Virus:

1. Inicie Faronics Core Console.
2. En el panel Console Tree (Árbol de la consola), vaya a *Faronics Core Console*>[Nombre de Core Server]>Workstations (Estaciones de trabajo)>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus.
3. Haga clic con el botón derecho en Anti-Virus y seleccione *Configure Anti-Virus (Configurar Anti-Virus)*.
4. Aparecerá la ficha Updates (Actualizaciones) en el diálogo Configure Faronics Anti-Virus (Configurar Faronics Anti-Virus).



5. La ficha Updates (Actualizaciones) muestra la versión del motor de análisis y la versión de definición de virus. Especifique las siguientes opciones:

Faronics Anti-Virus - Configurar

Actualizaciones | Servidor proxy

Versiones del anti-virus

Versión de definición de virus:

Actualizar configuración

☒ Actualizar automáticamente en: 4 horas

Verificar la configuración de las actualizaciones

Verificación de la fecha/hora de la última actualización: 25/05/2010 17:14:47 Actualizar ahora

Verificación de la fecha/hora de la próxima actualización: 25/05/2010 21:14:47

Estado de la actualización: de definición de virus no se actualiza.

Aceptar Cancelar

Configuración\Actualizaciones

- *Automatically update (in hours) (Actualizar automáticamente (en horas))*: seleccione la casilla de verificación para actualizar automáticamente las definiciones de virus.
 - *hours (horas)*: especifique un valor entre 1 a 77 horas.
 - *Update Now (Actualizar ahora)*: haga clic en este botón para actualizar las definiciones Anti-Virus.
6. Haga clic en la ficha Proxy Server (Servidor proxy) y especifique los valores de las siguientes opciones:

Faronics Anti-Virus - Configurar

Actualizaciones | Servidor proxy

☒ Use un servidor proxy para comunicarse con el servidor web de actualizaciones

Información del servidor proxy

Dirección: 192.168.1.01 Puerto:

Autenticación del usuario

☐ Mi servidor proxy requiere autorización (credenciales de inicio de sesión)

Tipo de autenticación: Basic

Nombre de usuario:

Contraseña:

Dominio:

Prueba

Aceptar Cancelar

Configuración\Servidor proxy

7. Seleccione Use a proxy server to communicate to Updates Web Server (Usar un servidor proxy para comunicarse con el Servidor Web de actualizaciones) y especifique la siguiente información:
- *Dirección*: especifique la dirección IP o URL.
 - *Puerto*: especifique el puerto.



8. Seleccione *Use a proxy server to communicate to Updates Web Server* (Usar un servidor proxy para comunicarse con el Servidor Web de actualizaciones) y especifique los siguientes ajustes:
 - *Tipo de autenticación*
 - *Nombre de usuario*
 - *Contraseña*
 - *Dominio*
9. Haga clic en *Test (Probar)* para probar la conexión. Haga clic en *OK (Aceptar)* para guardar la configuración del proxy.

Actualización de la configuración de Faronics Anti-Virus

Para obtener los ajustes de una sola estación de trabajo que esté ejecutando Faronics Anti-Virus, realice los siguientes pasos:

1. Inicie Faronics Core Console.
2. En el panel Console Tree (Árbol de la consola), vaya a *Faronics Core Console* > [Nombre de Core Server] > *Workstations (Estaciones de trabajo)* > *Managed Workstations (Estaciones de trabajo administradas)*.
3. Haga clic con el botón derecho del mouse en una estación de trabajo y seleccione *Refresh Anti-Virus (Actualizar configuración del Anti-Virus)*.
4. Faronics Anti-Virus se actualizará y se mostrarán las siguientes columnas actualizadas:
 - Nombre de la política
 - Estado
 - % del análisis completado
 - Versión de las definiciones
 - Fecha de la última actualización
 - Fecha del último análisis
 - Fecha de la última detección de una amenaza
 - Versión



Política de Faronics Anti-Virus

Una Política Anti-Virus contiene todos los ajustes de configuración acerca de cómo se ejecuta Faronics Anti-Virus en las estaciones de trabajo. Una política contiene la acción que se toma de acuerdo al programa, el calendario, los servidores proxy, los informes de errores y la funcionalidad permitida a los usuarios de las estaciones de trabajo. Las siguientes secciones explican cómo se crea y se aplica una política Anti-Virus.

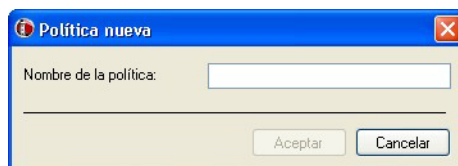


Faronics Anti-Virus contiene una política *Predeterminada*. La política Predeterminada contiene los ajustes de configuración más óptimos para administrar Faronics Anti-Virus.

Creación de políticas Anti-Virus

Realice los siguientes pasos para crear una nueva política Anti-Virus:

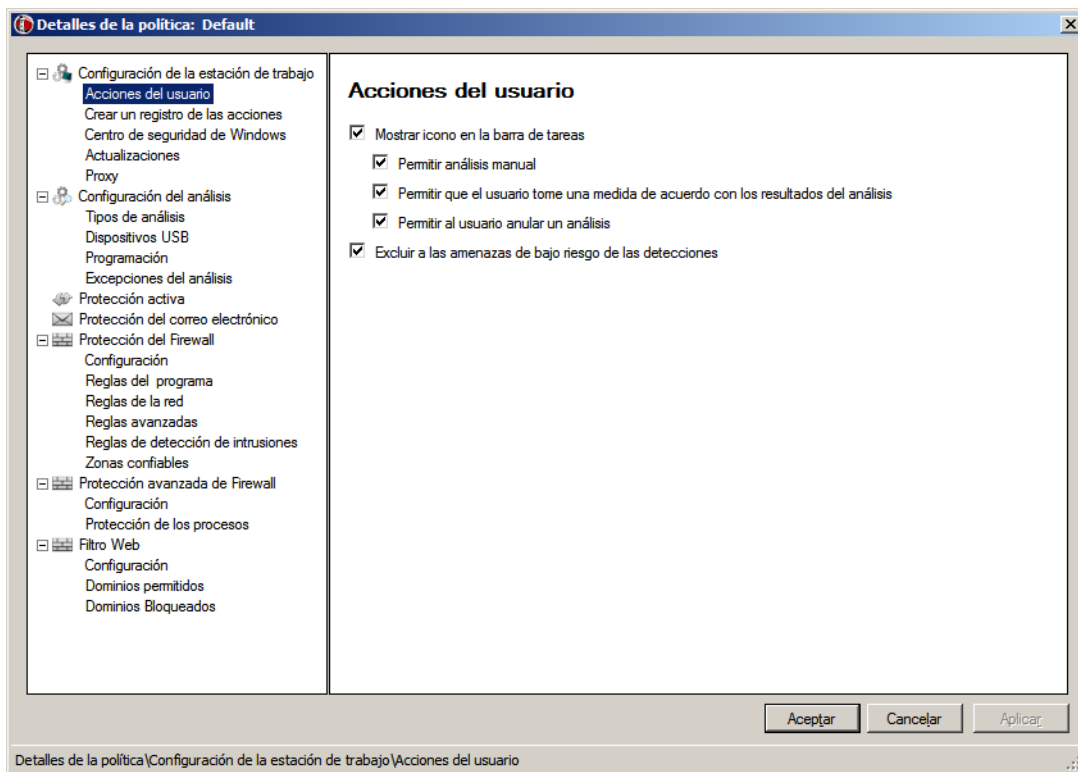
1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console > [Nombre de Core Server] > Workstations (Estaciones de trabajo) > Managed Workstations (Estaciones de trabajo administradas) > Anti-Virus*.
3. Haga clic con el botón derecho del mouse en *Anti-Virus* y seleccione *New Policy (Nueva política)*.
4. Especifique un nombre para la política en el diálogo *New Policy (Nueva política)*. Haga clic en *OK (Aceptar)*. Se crea una nueva política en el nodo *Anti-Virus* política. Por ejemplo, puede elegir como nombre de la política nueva *Política nueva 1*.



5. Haga clic con el botón derecho del mouse en *Política nueva 1* y seleccione *Policy Details (Detalles de la política)*. Se mostrará el diálogo *Policy Details (Detalles de la política)*.
6. Especifique los ajustes en el nodo *Workstation Settings (Ajustes de la estación de trabajo)* :



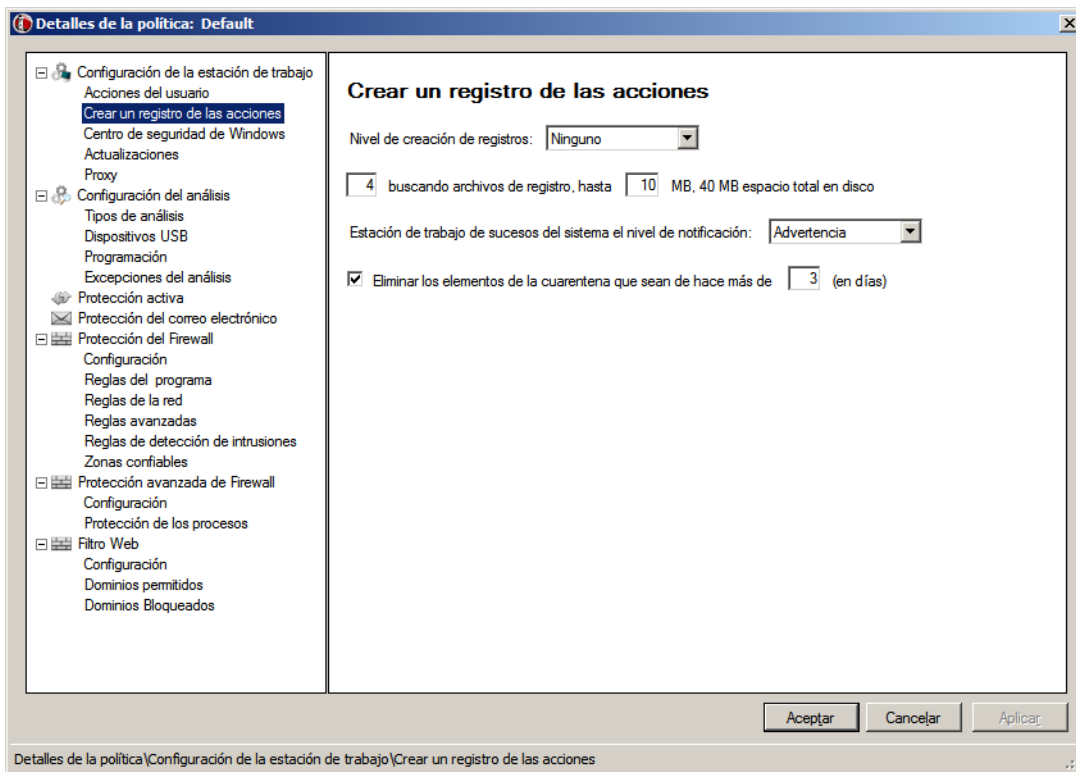
- Nodo *Workstation Settings* (*Ajustes de la estación de trabajo*) panel > *User Actions* (*Acciones del usuario*)



- *Show taskbar icon (mostrar icono en la barra de tareas)*: seleccione la casilla de verificación para mostrar el ícono de Faronics Anti-Virus en la barra de tareas en las estaciones de trabajo. Si esta casilla de verificación no está seleccionada, Faronics Anti-Virus estará oculto para el usuario.
- *Allow manual scanning (Permitir análisis manual)*: seleccione la casilla de verificación para permitir que los usuarios inicien manualmente el análisis de Faronics Anti-Virus en las estaciones de trabajo.
- *Allow user to take action on scan results (Permitir que el usuario tome una medida de acuerdo con los resultados del análisis)*: seleccione esta casilla de verificación para permitir que el usuario de la estación de trabajo tome medidas de acuerdo con los resultados del análisis.
- *Allow user to abort a scan initiated locally (Permitir al usuario anular un análisis iniciado localmente)*: seleccione la casilla de verificación para permitir que los usuarios anulen el análisis iniciado localmente en la estación de trabajo.
- *Exclude low risk threats from detections (Excluir a las amenazas de bajo riesgo de las detecciones)*: seleccione la casilla de verificación para excluir las amenazas de bajo riesgo de las detecciones. Amenazas de bajo riesgo se refiere a aquellas amenazas que no afectarán negativamente al sistema (por ejemplo, cookies).



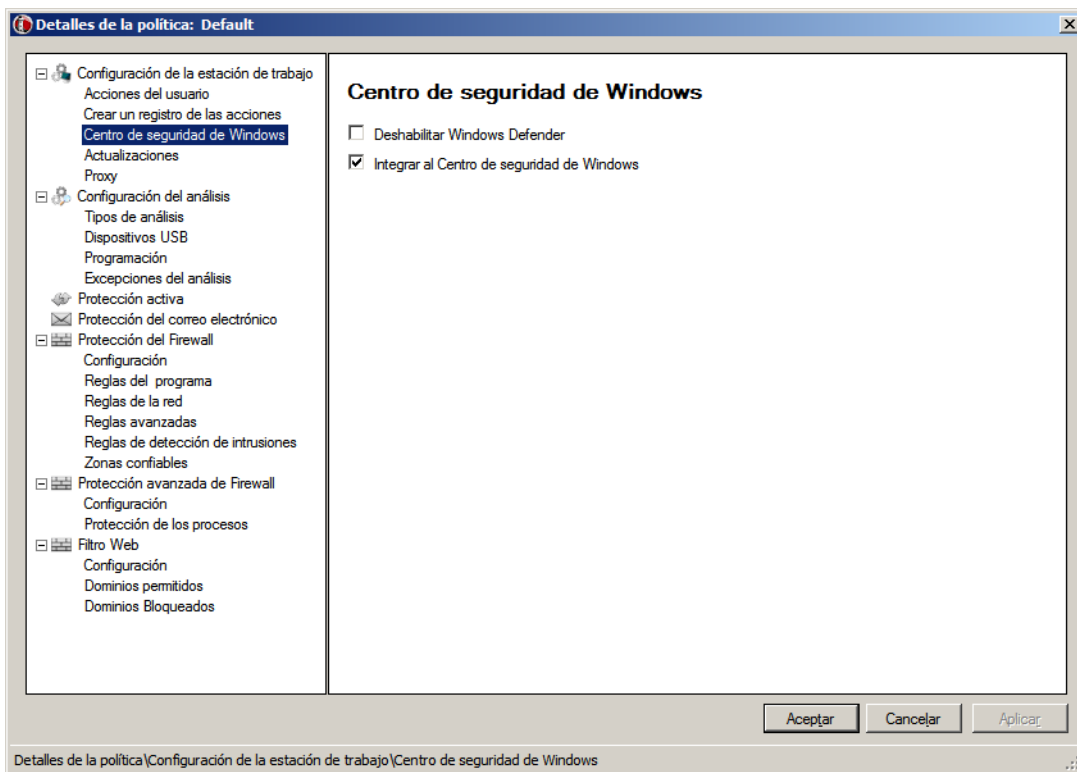
- Nodo *Workstation Settings (Ajustes de la estación de trabajo)* > *Log Actions (Crear un registro de las acciones)*



- *Logging Level (Nivel de creación de registros)*: seleccione el nivel de creación de registros. Seleccione *None (Ninguno)* para no crear ningún registro. Seleccione *Error* para crear un registro del mensaje de error. Seleccione *Trace (Rastro)* para el rastro. Seleccione *Verbose (Detallado)* para crear un registro detallado.
- *Number of logging files (Número de archivos de registro)*: especifique el número de archivos de registro. La información de creación de registros se almacena en archivos consecutivos. Por ejemplo, si hay 3 archivos A,B y C, Faronics Anti-Virus escribe primero los registros de errores en el archivo A. Una vez que el archivo A está lleno, comienza a escribir en el archivo B y finalmente en el archivo C. Una vez que el archivo C esté lleno, se borrarán los datos del archivo A y se escribirán allí los nuevos datos de registro.
- *File size (Tamaño del archivo)*: Seleccione el tamaño de cada archivo en MB.
- *Workstation system event report level (Nivel de informe de eventos del sistema de la estación de trabajo)*: Seleccione *None (Ninguno)*, *Error*, *Warning (Advertencia)* o *Information (Información)*.
- *Delete items from quarantine that are older than (Eliminar los elementos de la cuarentena que sean de hace más de)*: especifique el número de días para retener los elementos en cuarentena. El predeterminado es 3 días.



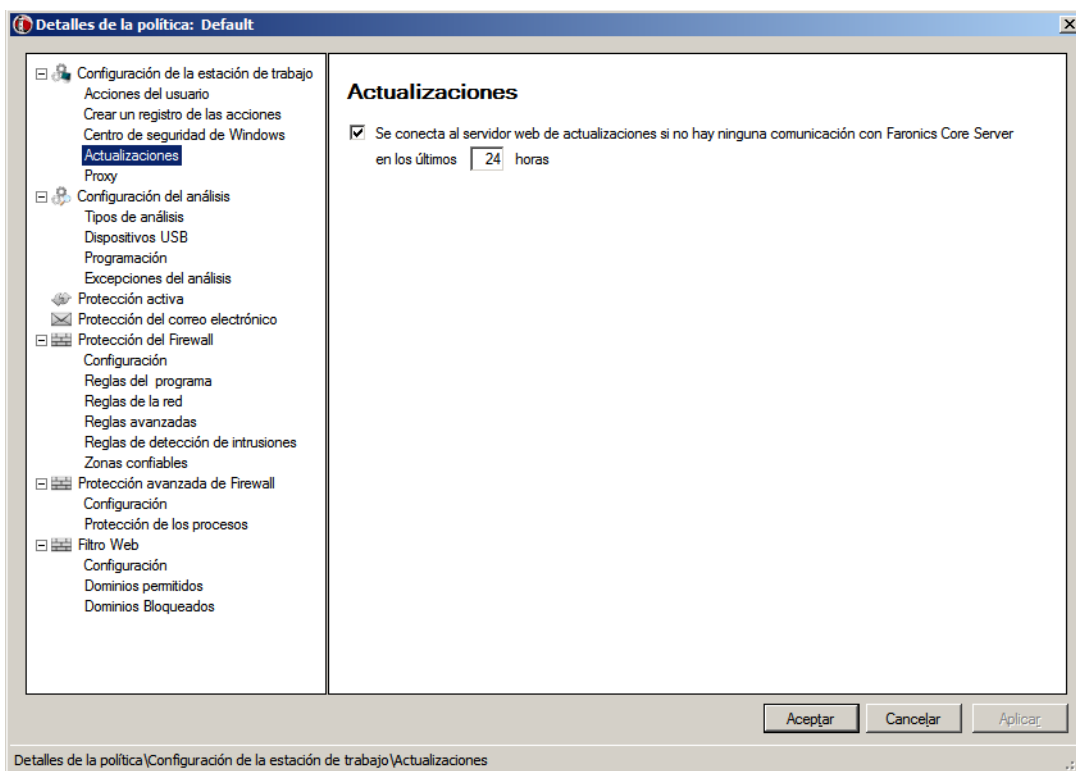
- Nodo *Workstation Settings (Ajustes de la estación de trabajo)* panel > *Windows Security Center*



- *Disable Windows Defender (Deshabilitar Windows Defender)*: seleccione esta casilla de verificación para deshabilitar Windows Defender. Esto evitará un posible conflicto entre Faronics Anti-Virus y Windows Defender. Ejecutar varios programas Anti-Virus o Anti-Spyware puede crear un conflicto porque un programa interpreta equivocadamente que el otro es un virus o spyware. Además, ejecutar varios programas Anti-Virus o Anti-Spyware puede aumentar el uso del procesador y la memoria. Sin embargo, si quiere seguir usando Windows Defender, puede elegir no deshabilitarlo.
- *Integrate into Windows Security Center (Integrar a Windows Security Center)*: seleccione la casilla de verificación para integrar Faronics Anti-Virus a Windows Security Center. Windows Security Center le notificará a través de la bandeja de sistema si Faronics Anti-Virus está activo o inactivo.



- *Nodo Workstation Settings (Ajustes de la estación de trabajo) > panel Updates (Actualizaciones)*



- *Connect to Updates Web Server if there is no communication with Faronics Core Server in the last x hours (Se conecta al servidor web de actualizaciones si no hay ninguna comunicación con Faronics Core Server en las últimas x horas):* seleccione la casilla de verificación para conectarse al servidor web de actualizaciones y descargar las definiciones de virus si la estación de trabajo pierde contacto con Faronics Core Server. Si no selecciona esta casilla de verificación, las definiciones de virus no se actualizarán si la estación de trabajo pierde la conexión con Faronics Core Server.



- *Nodo Workstation Settings (Ajustes de la estación de trabajo)> panelProxy*

Detalles de la política: Default

Proxy

Si su estación de trabajo requiere que un proxy se comunique con Faronics Core Server o con el servidor web de actualizaciones, configúrelos debajo.

☐ Habilitar proxy

Información del servidor proxy

Dirección: Puerto:

Autenticación del usuario

☐ Mi servidor proxy requiere autorización (credenciales de inicio de sesión)

Tipo de autenticación:

Nombre de usuario:

Contraseña:

Dominio:

Aceptar Cancelar Aplicar

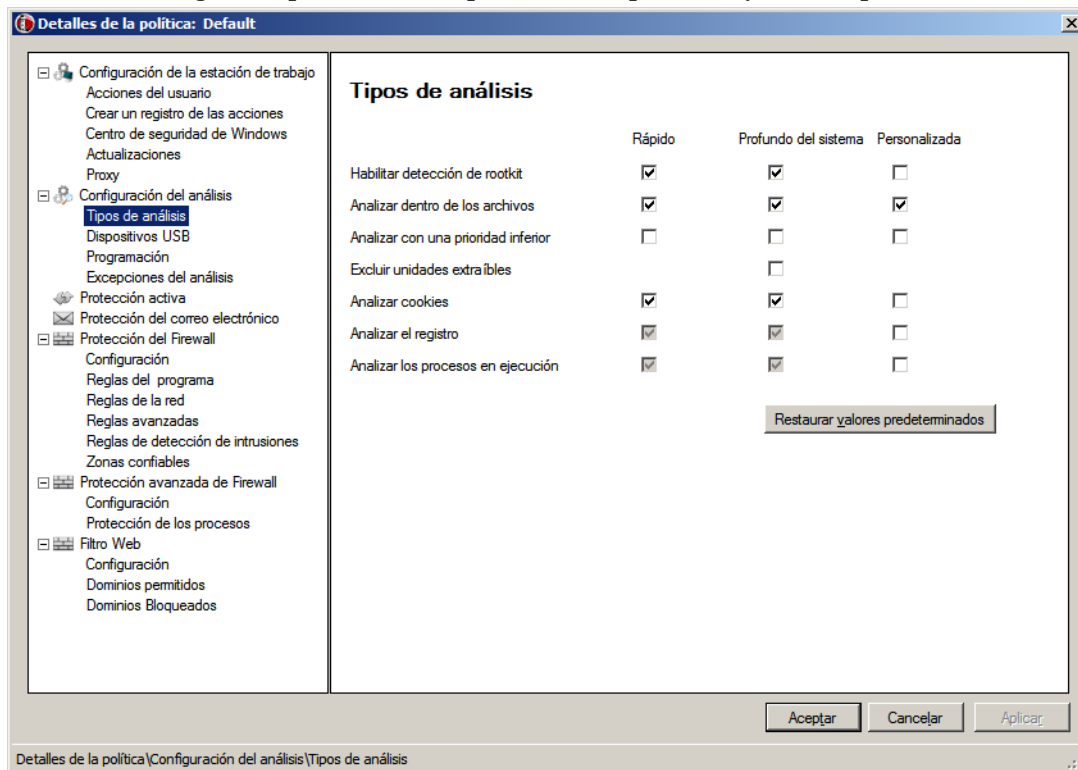
Detalles de la política\Configuración de la estación de trabajo\Proxy

- *Habilitar proxy*: seleccione la casilla de verificación si las estaciones de trabajo necesitan un proxy para comunicarse con Faronics Core Server o con el servidor web de actualizaciones. Especifique la *dirección* y el *puerto*.
- *Mi servidor proxy requiere autorización (credenciales de inicio de sesión)* : si el servidor requiere autenticación, especifique los valores para los siguientes campos:
- *Tipo de autenticación*: seleccione el tipo de autenticación.
 - *Nombre de usuario*: especifique el nombre de usuario.
 - *Contraseña*: especifique la contraseña.
 - *Dominio*: especifique el dominio.



7. Especifique los ajustes en el nodo *Scanning (Análisis)*:

- Nodo *Scanning (Análisis)* panel > *Scan Settings (Configuraciones de los análisis)* :
Seleccione lo siguiente para análisis rápido, análisis profundo y análisis personalizado:



Faronics Anti-Virus proporciona tres tipos de análisis:

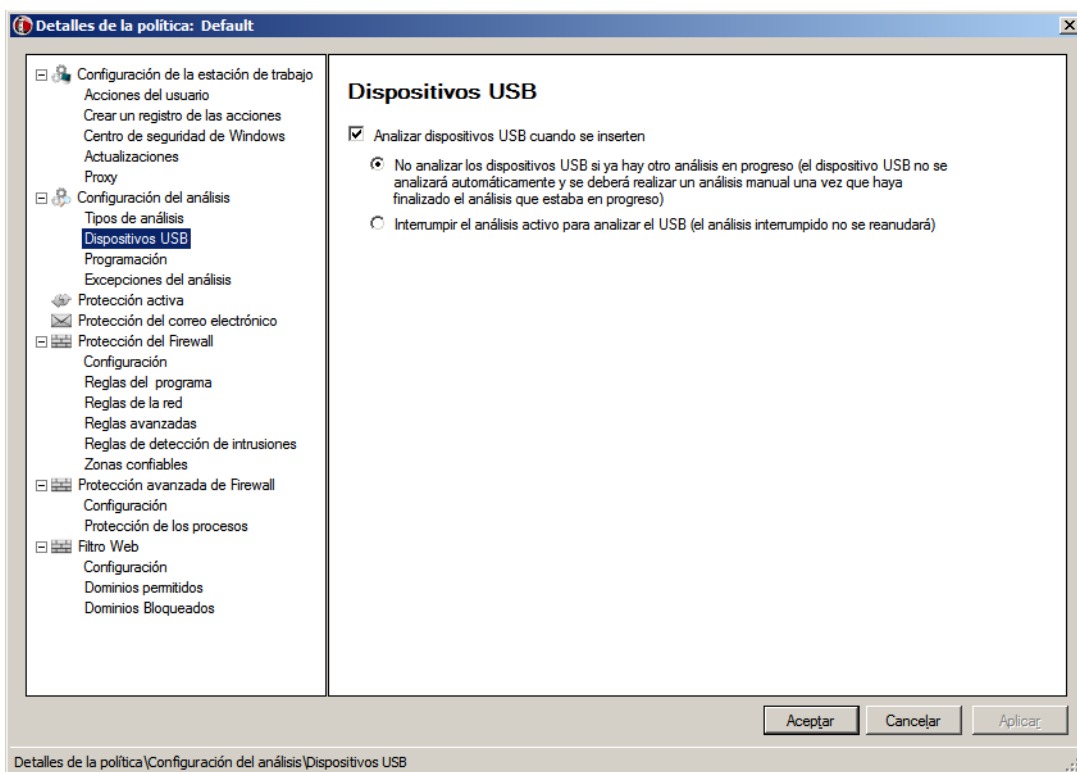
- *Análisis rápido*: analiza las áreas comúnmente afectadas de su computadora. Esto tiene menos duración que el análisis profundo del sistema. El análisis rápido también usa menos memoria que el análisis profundo del sistema.
- *Análisis profundo del sistema*: realiza un análisis minucioso de todas las áreas de la computadora. El tiempo que tarda el análisis depende del tamaño de su disco duro.
- *Análisis personalizado*: realiza un análisis de acuerdo con las selecciones que realizó en el diálogo *Detalles de la política*.

Para cada tipo de análisis, seleccione las siguientes opciones (algunas opciones pueden aparecer en color gris de acuerdo con el tipo de análisis):

- *Habilitar detección de rootkit*: detecta si la computadora está infectada con un rootkit.
- *Analizar dentro de los archivos*: analiza los contenidos de un archivo zip. Seleccione que el análisis incluya archivos comprimidos como .RAR y .ZIP. Cuando se detecta un archivo .RAR con un archivo infectado, el archivo .RAR se pondrá en cuarentena. Si se encuentra que el archivo .ZIP contiene un archivo infectado, el archivo infectado se pone en cuarentena y se reemplaza con un archivo .TXT con un texto que indica que estaba infectado y ha sido puesto en cuarentena.
- *Analizar con una prioridad inferior*: seleccione esta opción para operar Faronics Anti-Virus con una prioridad inferior, lo que le permite seguir trabajando con otros programas sin que disminuya el rendimiento. Es bueno seleccionar esta opción en el caso de los análisis programados que ocurren durante el uso regular del equipo.



- *Excluir unidades extraíbles (Ej. USB)* : excluye las unidades extraíbles del proceso de análisis. No se analizará ningún disco duro externo o unidad USB.
- *Analizar cookies*: analiza los archivos cookies guardados en la estación de trabajo.
- *Analizar el registro*: analiza el registro.
- *Analizar procesos en ejecución*: analiza todos los procesos en ejecución.
- *Nodo Analizando*> panel *Dispositivos USB* - Especificar la siguiente configuración:



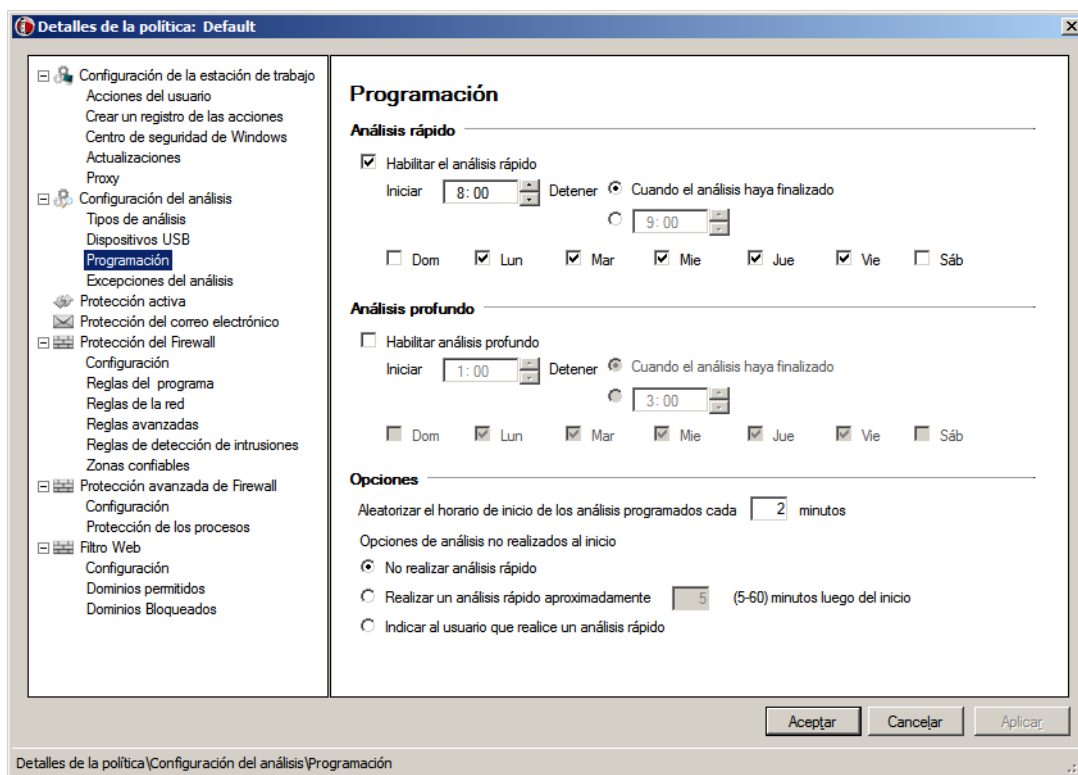
- *Analizar las unidades USB al insertarlas* - seleccione la casilla de verificación para analizar las unidades USB cuando se inserten y seleccione una de las siguientes opciones:
 - *No realizar el análisis del dispositivo USB si ya hay otro análisis en progreso*: seleccione esta opción para garantizar que no se interrumpa un análisis activo cuando se inserte una unidad USB. La unidad USB se deberá analizar manualmente una vez que haya finalizado el análisis activo.
 - *Interrumpir el análisis activo para realizar el análisis del dispositivo USB*: seleccione esta opción para interrumpir un análisis activo y analizar la unidad USB cuando se inserte. Una vez que el análisis activo se interrumpe, no se reanudará automáticamente y habrá que reiniciarlo manualmente.



Si la casilla de selección *Permitir análisis manual* está seleccionada en la ficha *Configuración de la estación de trabajo* panel >*Acciones del usuario*, el dispositivo USB se analizará automáticamente. Si la casilla de verificación *Permitir análisis manual* no está seleccionada, el dispositivo USB no se analizará automáticamente.



- Nodo *Scanning (Analizando)* panel > *Schedule (Programar)*: especifique la siguiente configuración:



Análisis rápido:

- *Habilitar el análisis rápido*: seleccione la casilla de verificación para habilitar el análisis rápido.
- *Inicio*: especifique la hora de inicio.
- *Fin*: especifique la hora de finalización. La duración máxima entre la hora de *Inicio* y *Finalización* es de 23.59 horas. El análisis finaliza si se analizaron todos los archivos antes de la hora de *Finalización*. Si el análisis no se completó antes de la hora de *Finalización*, se anula en la hora de *Finalización*. Como alternativa, seleccione *Cuando el análisis haya finalizado* para asegurarse de que se complete el análisis.
- *Días*: seleccione los días en los que se realizará el análisis rápido.

Análisis profundo:

- *Habilitar el análisis profundo*: seleccione la casilla de verificación para habilitar el análisis profundo.
- *Inicio*: especifique la hora de inicio.
- *Fin*: especifique la hora de finalización. La duración máxima entre la hora de *Inicio* y *Finalización* es de 23.59 horas. El análisis finaliza si se analizaron todos los archivos antes de la hora de *Finalización*. Si el análisis no se completó antes de la hora de *Finalización*, se anula en la hora de *Finalización*. Como alternativa, seleccione *Cuando el análisis haya finalizado* para asegurarse de que se complete el análisis.
- *Días*: seleccione los días en los que se realizará el análisis profundo.



Opciones:

- *Aleatorizar el horario de inicio de los análisis programados cada x minutos*: especifique el número de minutos. La hora de inicio del análisis programado se aleatoriza para reducir el impacto en el tráfico de la red. Faronics Anti-Virus informa a Faronics Core cuando se inicia el análisis. Esto puede tener un impacto en el tráfico de la red si se analizan varios sistemas al mismo tiempo.

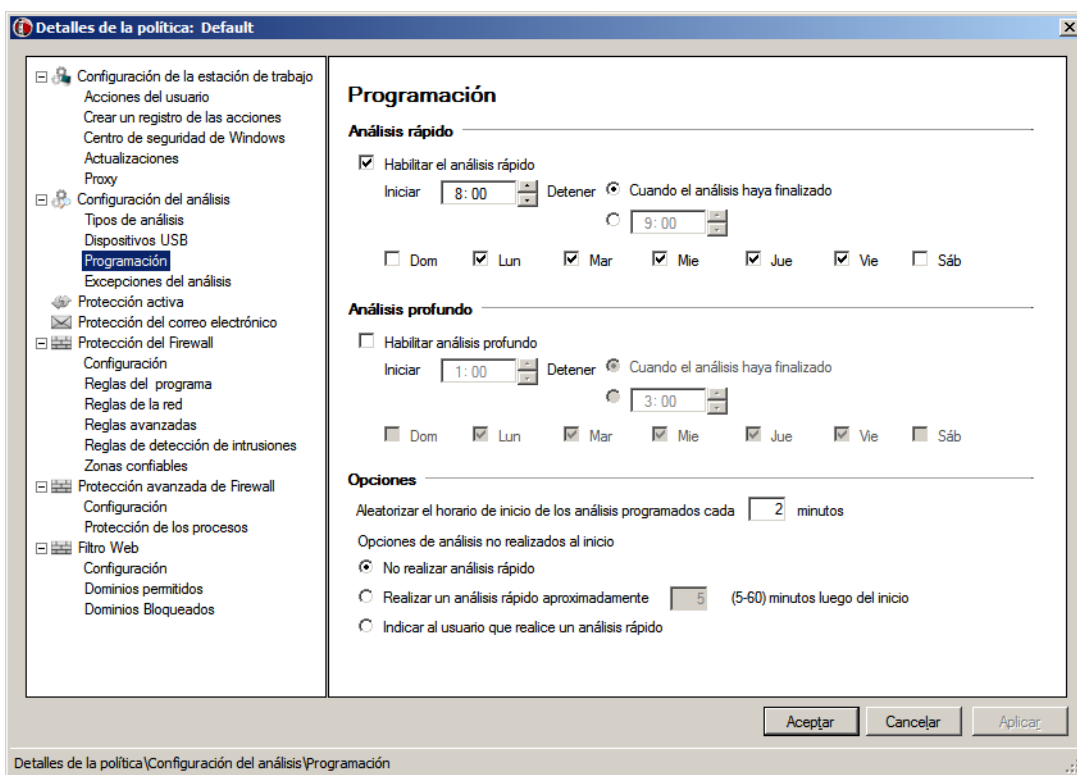
Opciones de análisis no realizados al inicio: Seleccione una de las siguientes opciones de cómo se realizará un análisis si la estación de trabajo no estaba *ENCENDIDA* durante un análisis programado:

- *No realizar análisis rápido*: seleccione esta opción si no desea realizar el análisis rápido cuando se inicie el equipo.
- *Realizar un análisis rápido aproximadamente x minutos luego del inicio*: especifique el número de minutos luego del inicio para que Faronics Anti-Virus realice un análisis rápido.
- *Indicar al usuario que realice un análisis rápido*: seleccione la opción para indicarle al usuario que realice un análisis rápido.

8. Especifique los ajustes en el nodo *Scanning (Análisis) > Scan Exceptions (Excepciones del análisis)*:

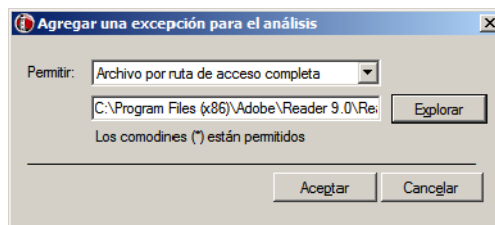
Las carpetas o los archivos que se sabe que son seguros y están libres de infecciones se pueden agregar a la ficha Scan Exceptions (Excepciones del análisis). Las carpetas o los archivos agregados a la ficha Scan Exceptions (Excepciones del análisis) siempre serán analizados por Faronics Anti-Virus. Sin embargo, Faronics Anti-Virus nunca informará que los archivos son maliciosos o están infectados. Esta función es útil debido a que los archivos y las carpetas que el administrador sabe que son seguros no serán informados como maliciosos.

- Haga clic en *Add (Agregar)*.

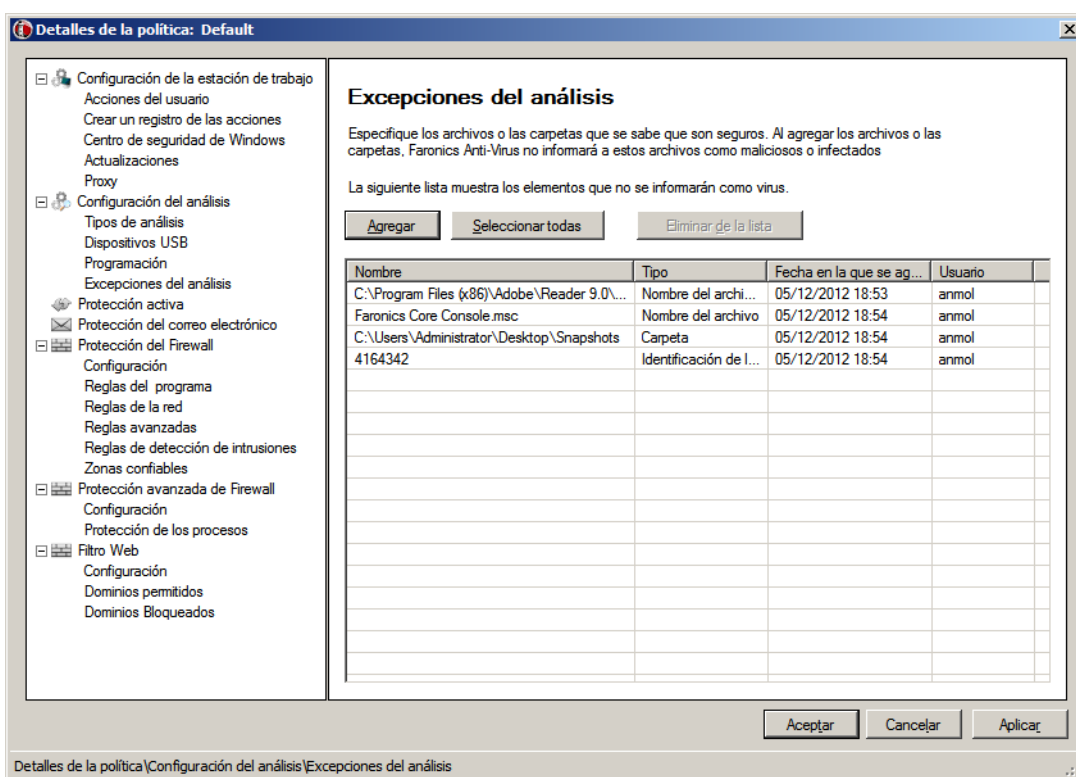




- b. En el diálogo *Add (Agregar)*, seleccione *File by full path (Archivo por ruta de acceso completa)*, *File by name only (Archivo sólo por nombre)* o *Entire folder (Carpeta completa)*. Haga clic en *Browse (Buscar)* para seleccionar la carpeta y haga clic en *OK*.

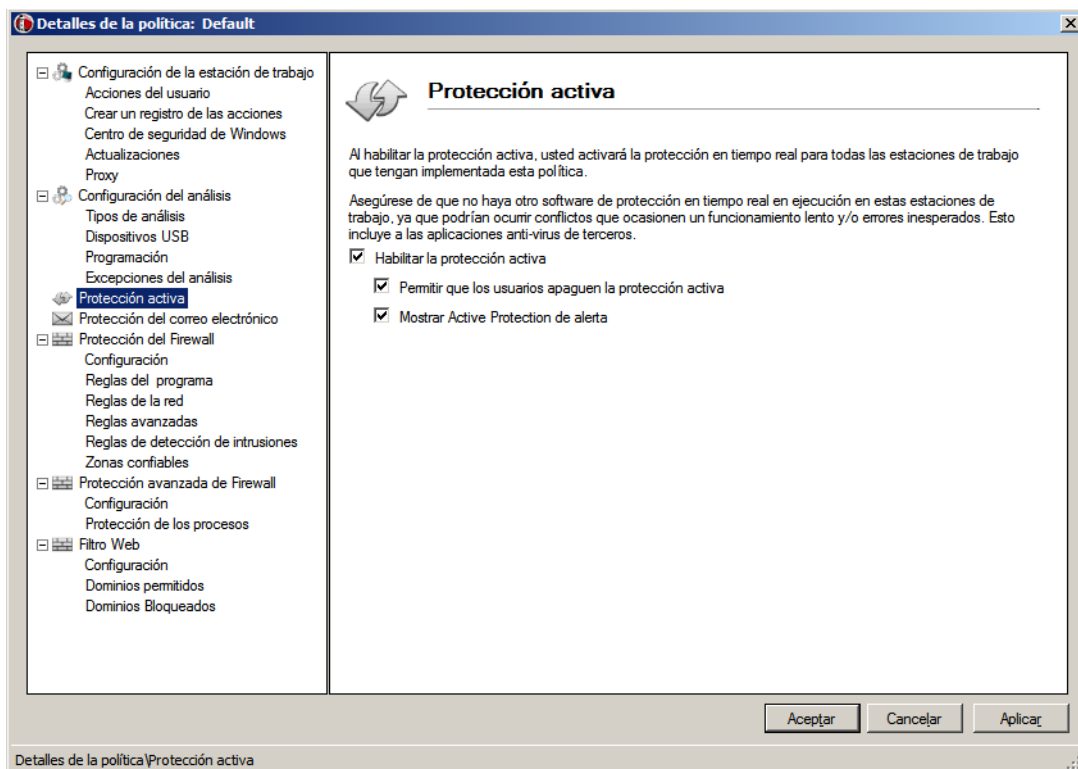


- c. *File by full path (Archivo por ruta de acceso completa)* se agregará al panel *Scan Exceptions (Excepciones del análisis)*.





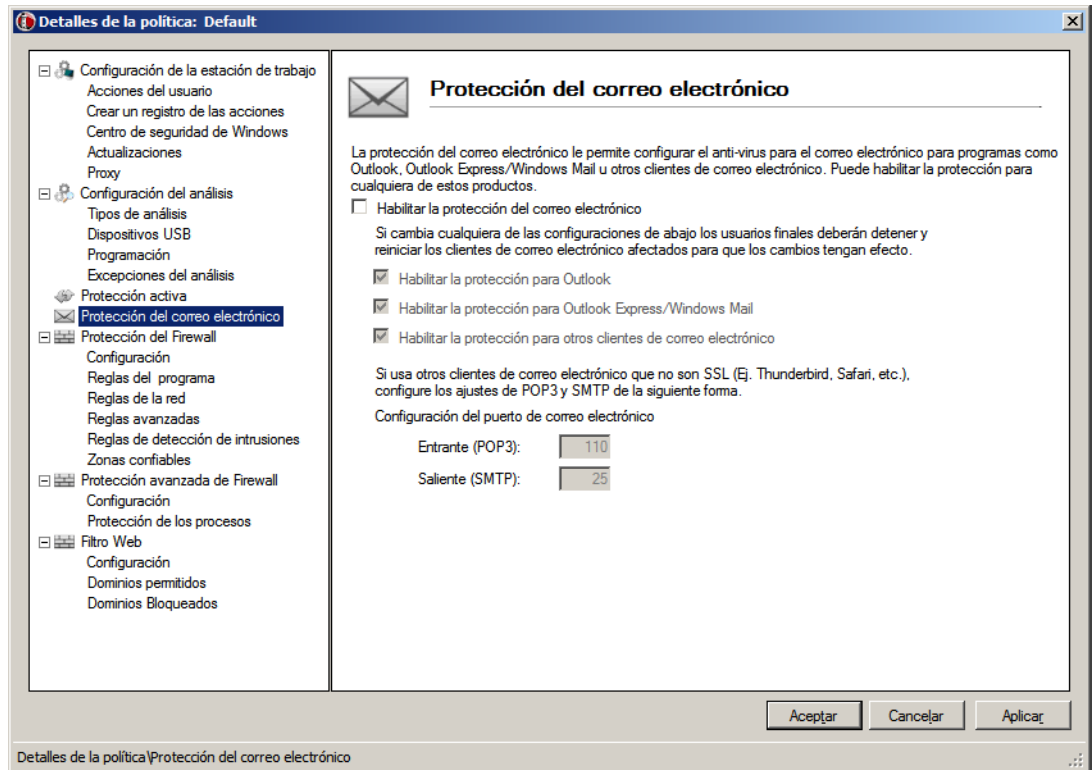
9. Especifique los ajustes en el panel *Active Protection (Protección activa)* :



- **Habilitar la protección activa:** seleccione esta opción para habilitar la protección en tiempo real. La protección activa es el análisis en tiempo real de Faronics Anti-Virus en segundo plano sin ningún impacto en el rendimiento del sistema. Si hay un riesgo de infección de virus en tiempo real de Internet, seleccione esta opción.
- **Permitir que los usuarios apaguen la protección activa:** seleccione esta opción para permitir a los usuarios apagar la protección activa. Si los usuarios instalan o usan software que podría confundirse con un virus (por ejemplo, macros avanzadas en Microsoft Office o lotes de archivos complejos), seleccione esta opción.
- **Show Active Protection alert (Mostrar alerta de protección activa):** seleccione esta opción para mostrar una alerta si se detecta una amenaza durante la protección activa. No seleccione esta casilla de verificación si no desea que se muestre un alerta.



10. Especifique los ajustes en el panel *Email Protection (Protección de correo electrónico)* :



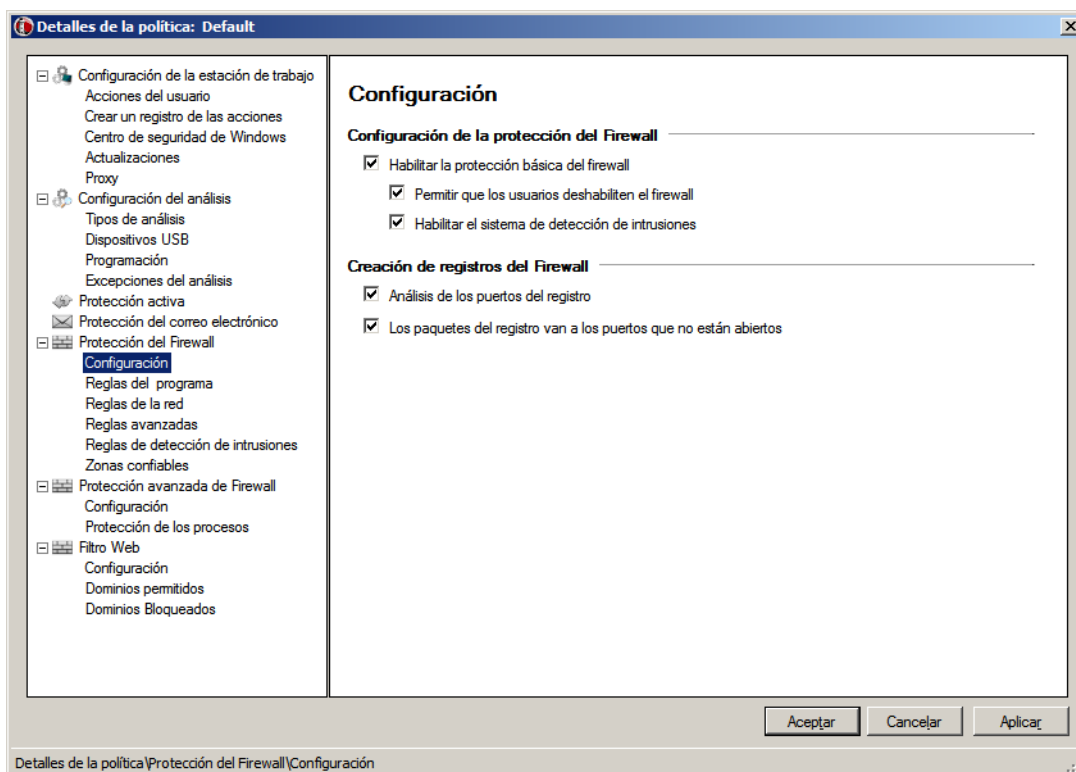
- *Habilitar la protección del correo electrónico:* seleccione la casilla de verificación para habilitar la protección del correo electrónico. Las siguientes opciones se habilitan si se encuentra seleccionado *Habilitar la protección del correo electrónico*.
 - *Habilitar la protección para Outlook:* seleccione la casilla de verificación para habilitar la protección para Outlook. Faronics Anti-Virus analiza todos los mensajes de correo electrónico entrantes y salientes de Outlook.
 - *Habilitar la protección para Outlook Express/Windows Mail:* seleccione la casilla de verificación para habilitar la protección para Outlook Express/Windows Mail. Faronics Anti-Virus analiza todos los mensajes de correo electrónico entrantes y salientes de Outlook/Windows Mail.
 - *Habilitar la protección para otros clientes de correo electrónico:* especifique la configuración de los puertos de correo electrónico para el correo entrante (POP3) y el correo saliente (SMTP). Faronics Anti-Virus analiza todos los mensajes de correo electrónico de los programas de correo electrónico con las configuraciones de correo *Entrante y Saliente*.



11. Especifique los ajustes en el nodo *Firewall Protection (Protección del Firewall)*:

El nodo Firewall proporciona protección bidireccional que lo protege del tránsito entrante y saliente. Puede crear reglas personalizadas para proteger su red. Puede *Permitir* o *Bloquear* la comunicación y también configurar el Firewall para que le *Pregunte*.

- *Panel de Configuración* del nodo Firewall



Configuración de la protección del Firewall:

- Seleccione la casilla *Enable basic firewall protection (Habilitar la protección básica del firewall)* para habilitar la protección del firewall.
- *Les permite a los usuarios deshabilitar el firewall* - Esta casilla de verificación está habilitada si se selecciona *Enable basic firewall protection (Habilitar la protección básica del firewall)*. Al seleccionar esta opción los usuarios podrán deshabilitar el firewall en la estación de trabajo.

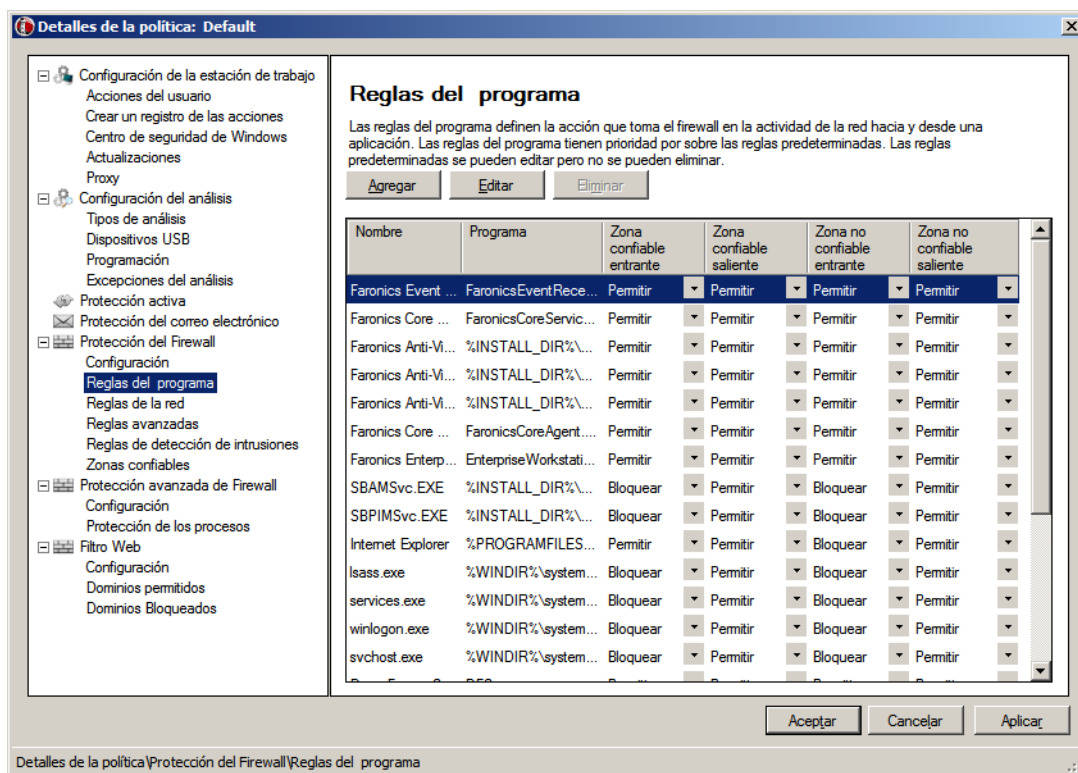
Creación de registros del Firewall:

- *Registre los paquetes que salen por los puertos que no están abiertos* - Seleccione la casilla de verificación para registrar los paquetes de datos que salen por los puertos que no están abiertos. Estos datos son útiles para analizar los intentos de comunicación con puertos que no están abiertos en la red.
- *Registrar los análisis de los puertos* - Seleccione la casilla de verificación para registrar todos los intentos de analizar los puertos a través de la red. Los datos de análisis de puertos se guardarán en el archivo de registro.



- **Nodo Firewall Protection (Protección del Firewall) > panel *Program Rules (Reglas del programa)***

Las reglas del programa definen la acción que toma el firewall en la actividad de la red hacia y desde una aplicación. Las reglas del programa tienen prioridad por sobre las reglas predeterminadas. Las reglas predeterminadas se pueden editar pero no se pueden eliminar.



Haga clic en **Add (Agregar)** para agregar una regla de programa nueva. Especifique o seleccione las opciones y haga clic en **OK (Aceptar)**. Se mostrarán los siguientes parámetros:

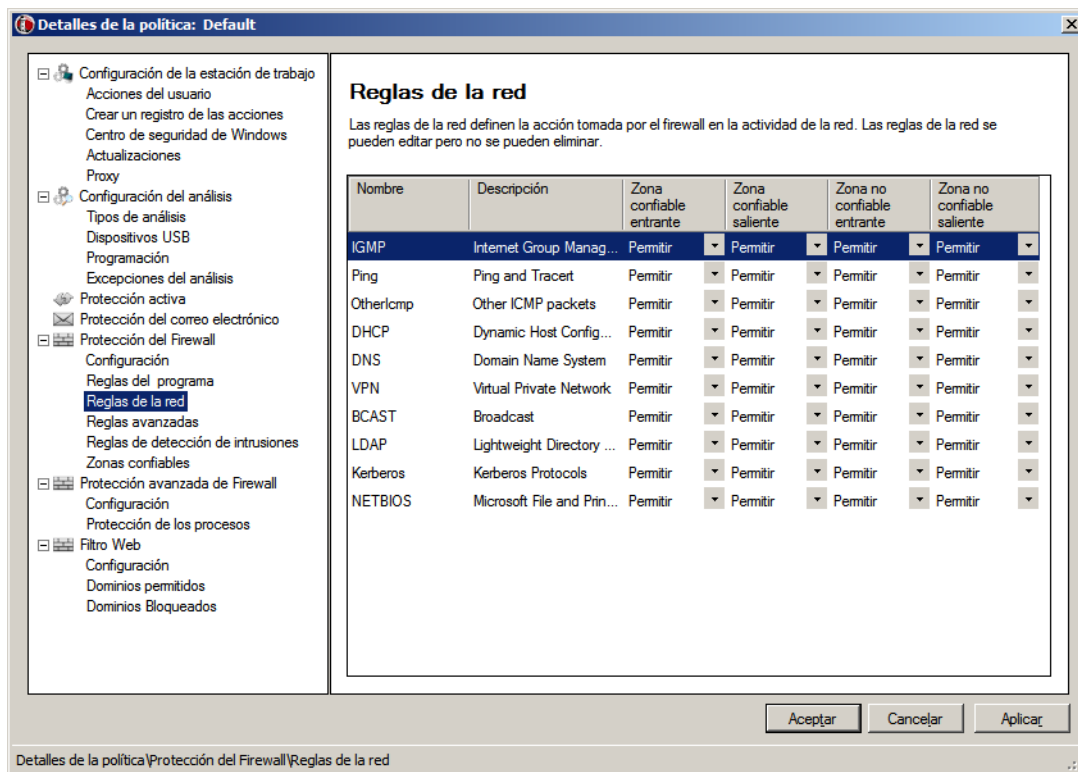


- *Nombre*: el nombre de la regla.
- *Programa*: el nombre del programa, incluida la ruta de acceso completa y la extensión.
- *Zona confiable entrante*: la acción que se debe tomar para las comunicaciones entrantes al programa en una Zona confiable (*Permitir*, *Bloquear* o *Preguntar*).
- *Zona confiable saliente*: la acción que se debe tomar para las comunicaciones salientes del programa en una Zona confiable (*Permitir*, *Bloquear* o *Preguntar*).
- *Zona no confiable entrante*: la acción que se debe tomar para las comunicaciones entrantes al programa en una Zona no confiable (*Permitir*, *Bloquear* o *Preguntar*).
- *Zona no confiable saliente*: la acción que se debe tomar para las comunicaciones salientes del programa en una Zona no confiable (*Permitir*, *Bloquear* o *Preguntar*).



- **Nodo Firewall Protection (Protección del Firewall) > panel Network Rules (Reglas de la red)**

Las reglas de la red definen la acción tomada por el firewall en la actividad de la red. Las reglas de la red se pueden editar pero no se pueden eliminar.



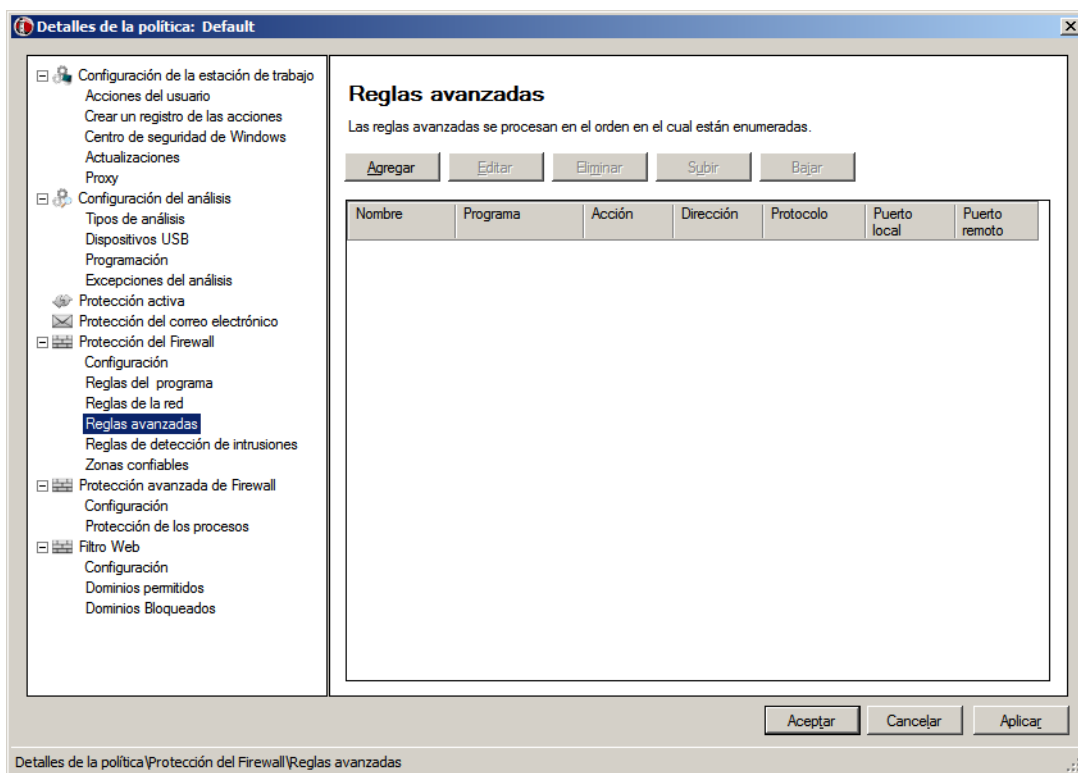
Se mostrarán los siguientes parámetros:

- **Nombre:** el nombre del protocolo.
- **Descripción:** la descripción del protocolo.
- **Zona confiable entrante:** la acción que se debe tomar para las comunicaciones entrantes al protocolo en una Zona confiable (*Permitir*, *Bloquear* o *Preguntar*).
- **Zona confiable saliente:** la acción que se debe tomar para las comunicaciones salientes del protocolo en una Zona confiable (*Permitir*, *Bloquear* o *Preguntar*).
- **Zona no confiable entrante:** la acción que se debe tomar para las comunicaciones entrantes al protocolo en una Zona no confiable (*Permitir*, *Bloquear* o *Preguntar*).
- **Zona no confiable saliente:** la acción que se debe tomar para las comunicaciones salientes del protocolo en una Zona no confiable (*Permitir*, *Bloquear* o *Preguntar*).

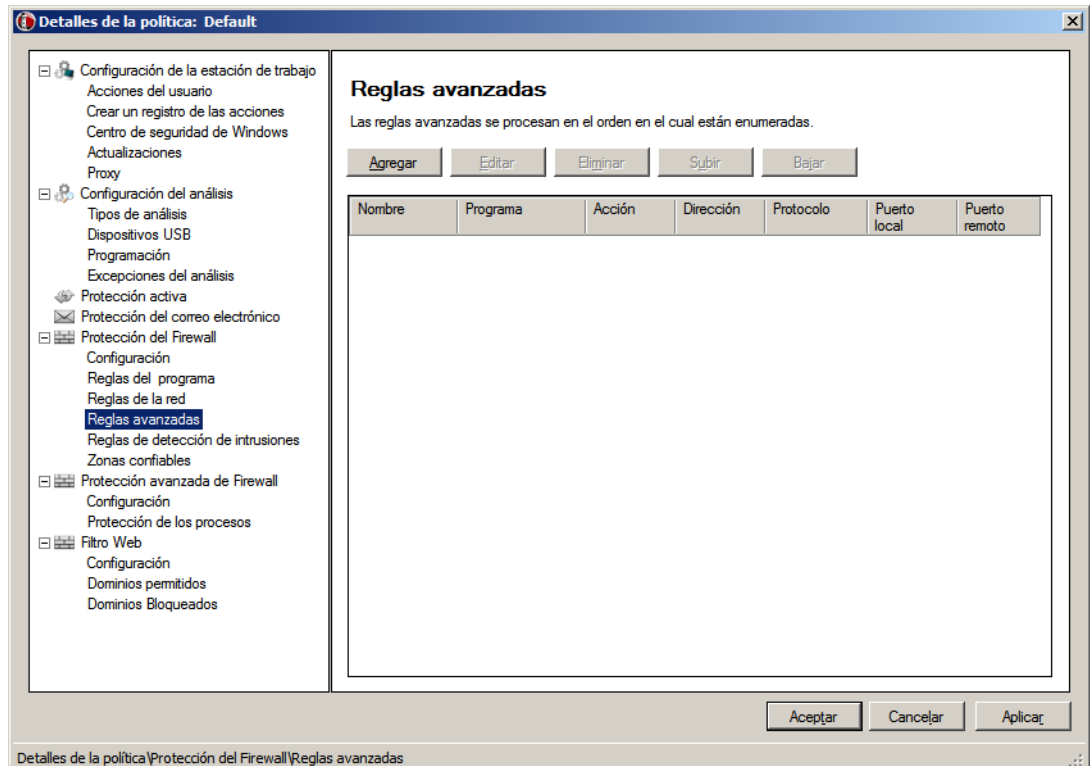


- *Nodo Firewall Protection (Protección del Firewall) > panel Advanced Rules (Reglas avanzadas)*

Las reglas avanzadas definen la acción que toma el firewall para la aplicación, el puerto o el protocolo especificado. Esto puede incluir un protocolo simple o un protocolo combinado, puertos locales o remotos, y la dirección del tránsito. Puede agregar, editar o eliminar una regla avanzada.



Haga clic en *Add (Agregar)* para agregar una regla avanzada nueva. Especifique o seleccione las opciones y haga clic en *OK (Aceptar)*. Se muestran los siguientes parámetros en el panel Reglas avanzadas:



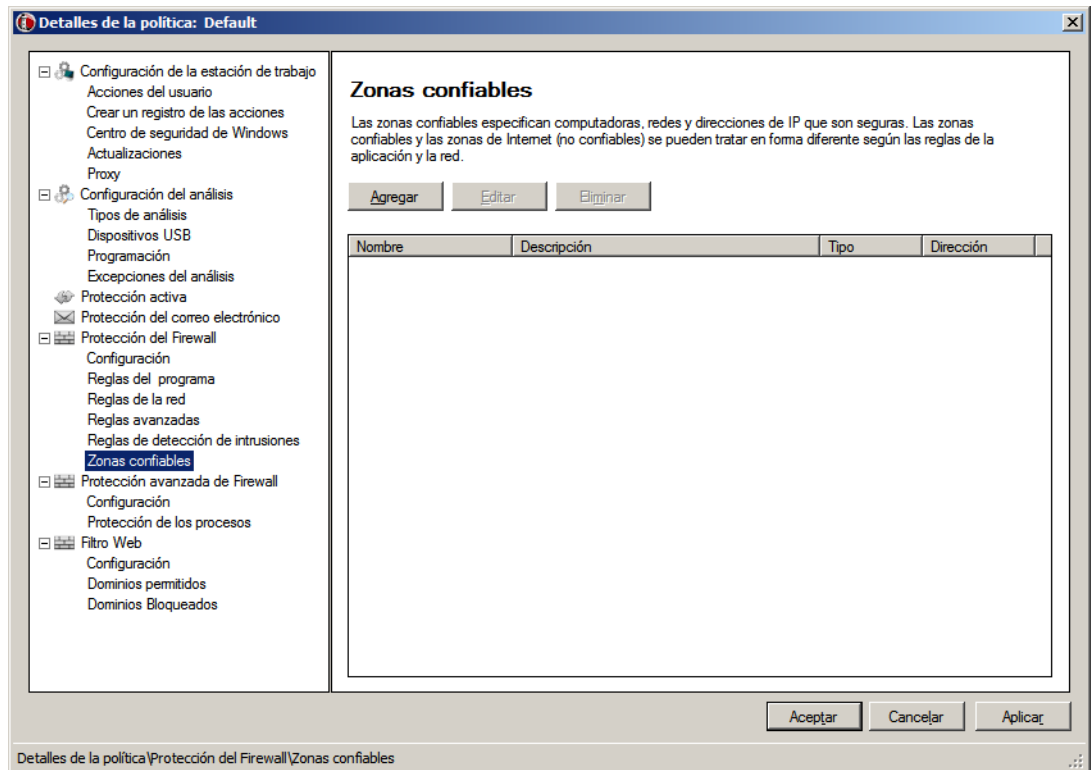
- **Nombre:** el nombre de la regla.
- **Programa:** el nombre del programa y la ruta de acceso.
- **Acción:** la acción tomada por el Firewall para la comunicación desde la aplicación, el puerto o el protocolo especificado (*Permitir, Bloquear o Preguntar*).
- **Dirección:** la dirección de la comunicación (*Ambas, Entrante, Saliente*).
- **Protocolo:** el nombre del protocolo.
- **Puerto local:** detalles del puerto local.
- **Puerto remoto:** detalles del puerto remoto.



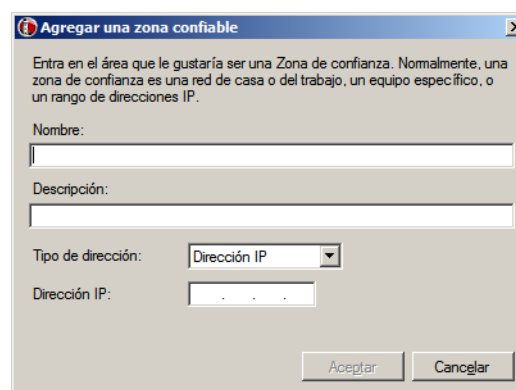
- *Nodo Firewall Protection (Protección del Firewall) > panel Trusted Zones (Zonas confiables)*

Las Zonas confiables especifican computadoras, redes y direcciones de IP que son confiables.

Las zonas confiables y las zonas de Internet (no confiables) se pueden tratar en forma diferente según las reglas de la aplicación y la red.



Haga clic en *Add (Agregar)* para agregar una zona confiable nueva. Especifique o seleccione las opciones y haga clic en *OK (Aceptar)*. Se mostrarán los siguientes parámetros:

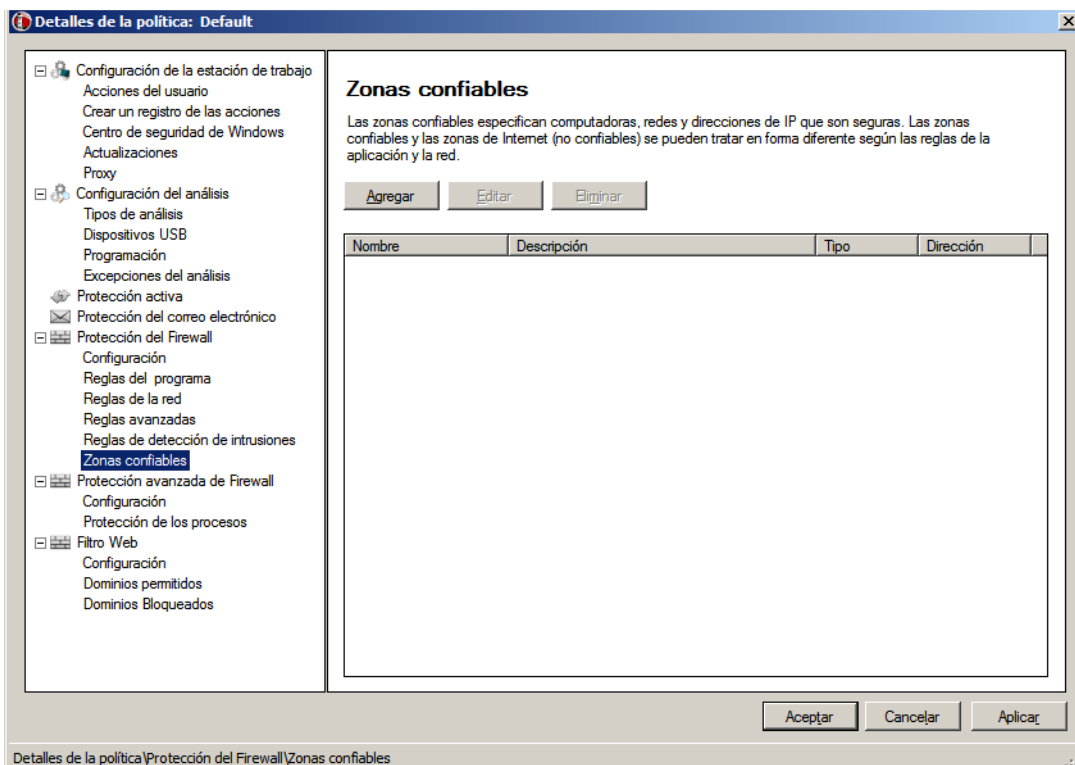


- *Nombre*: el nombre de la Zona confiable.
- *Descripción*: la descripción de la Zona confiable.
- *Tipo*: el tipo de la Zona confiable (*Dirección de IP, Rango de direcciones o Red*).

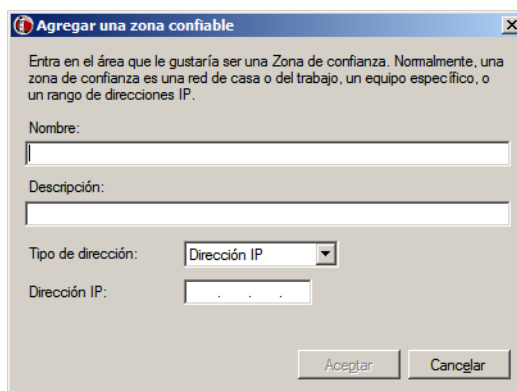


- *Nodo* Protección del Firewall > panel El sistema de detección de intrusiones

El sistema de detección de intrusiones (Intrusion Detection System, IDS) se usa para permitir o bloquear la actividad de la red sobre la base de una regla de intrusión definida. Especifique la acción (Permitir o Bloquear) en el panel de Reglas de detección de intrusiones para cada regla que esté categorizada como prioridad Alta, Media o Baja en esta pantalla. Haga clic en *Editar* para editar o *Eliminar* para eliminar una regla pre-existente.



Haga clic en *Agregar* para agregar una regla de detección de intrusión nueva. Especifique o seleccione las opciones y haga clic en *Aceptar*. Los siguientes parámetros se mostrarán cuando haga clic en *Agregar*:

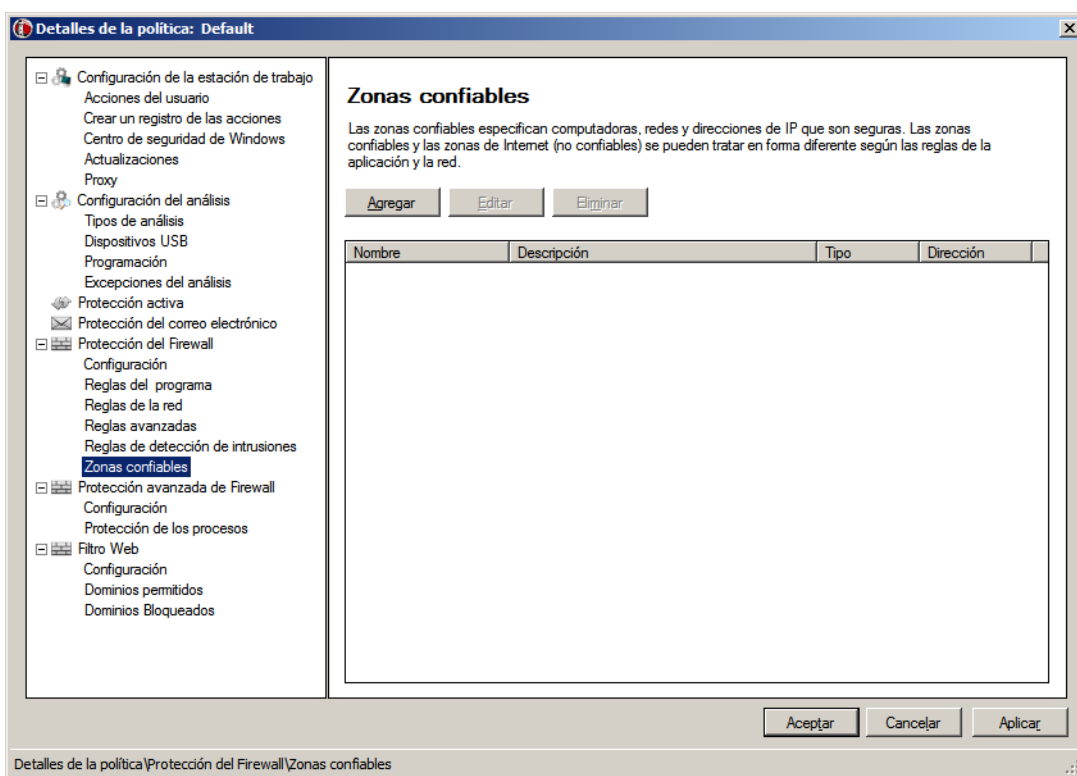




- **Habilitado:** seleccione esta opción si esta regla se habilitará.
- **Prioridad:** seleccione si la prioridad es *Alta*, *Media* o *Baja*.
- **Categoría:** seleccione la categoría (como *malo-desconocido*, *intento-admin*, *intento-dos*, o *intento-recon*).
- **Regla de Snort:** especifique la regla de snort. Para obtener más información acerca de las reglas de Snort, visite www.snort.org/snort/faq.

- **Nodo Protección del Firewall > panel Zonas confiables**

Las Zonas confiables especifican computadoras, redes y direcciones de IP que son confiables. Las zonas confiables y las zonas de Internet (no confiables) se pueden tratar en forma diferente según las reglas del programa y de la red.



Haga clic en **Agregar** para agregar una zona confiable nueva. Especifique o seleccione las opciones y haga clic en **Aceptar**. Se mostrarán los siguientes parámetros:



- *Nombre*: el nombre de la Zona confiable.
 - *Descripción*: la descripción de la Zona confiable.
 - *Tipo*: el tipo de la Zona confiable (*Dirección de IP*, *Rango de direcciones* o *Red*).
- *Nodo Protección del Firewall* > panel *Configuración*
- El panel Configuración le permite habilitar o deshabilitar la protección de procesos y la protección al inicio.

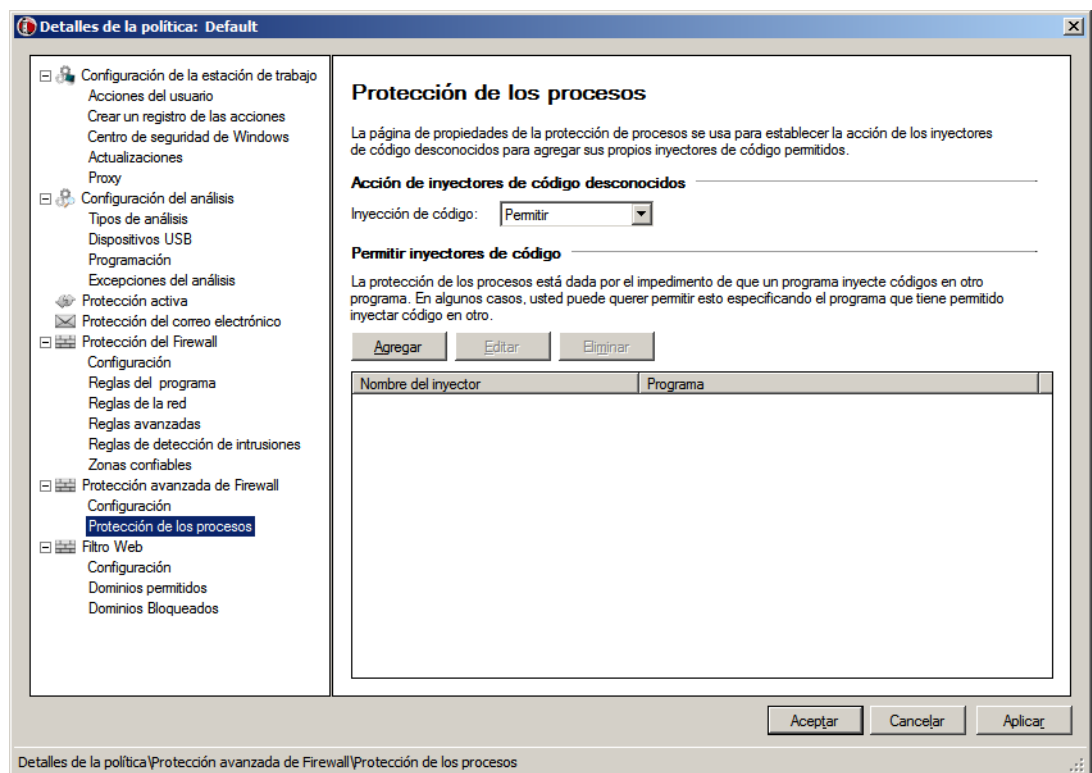


Seleccione las opciones y haga clic en *Aplicar*. Se mostrarán los siguientes parámetros:

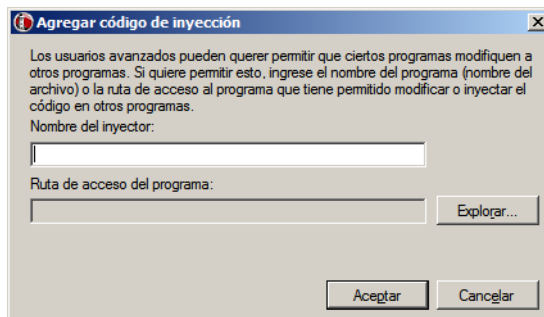
- *Habilitar protección de procesos*: seleccione esta opción para habilitar la protección de los procesos. Esta función se usa para establecer la acción ante inyectores de código desconocidos y para agregar sus propios inyectores de códigos permitidos de acuerdo con la configuración en el panel *Protección de procesos*.
- *Habilitar protección al inicio*: seleccione esta opción para habilitar la protección al inicio. La protección al inicio protege a su computadora cuando se inicia, bloquea el tráfico que pueda ocurrir antes de que Windows tenga una oportunidad de abrirse.

- *Nodo Protección del Firewall > panel Protección de procesos*

La página de propiedades de la protección de procesos se usa para establecer la acción de los inyectores de código desconocidos para agregar sus propios inyectores de código permitidos. La protección de los procesos está dada por el impedimento de que un programa inyecte códigos en otro programa. En algunos casos, usted puede querer permitir esto especificando el programa que tiene permitido inyectar código en otro.



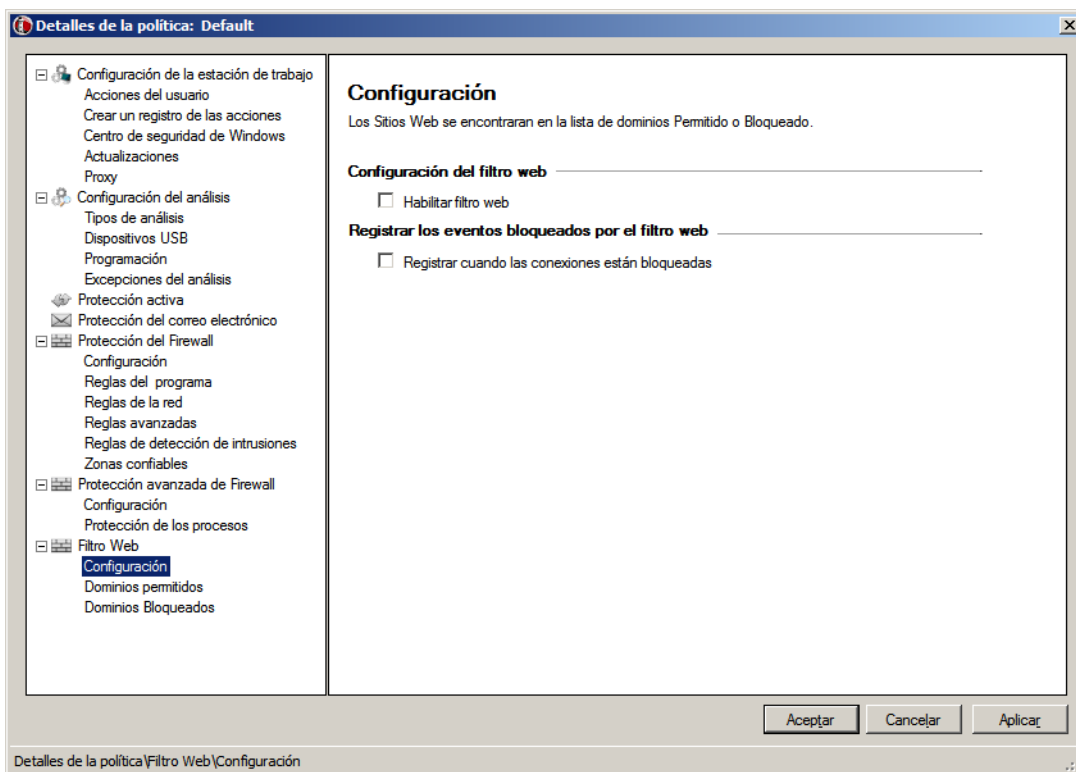
Haga clic en *Agregar* para agregar un nuevo inyector de código. Especifique o seleccione las opciones y haga clic en *Aceptar*. Se mostrarán los siguientes parámetros:



- *Nombre del inyector:* especifique el nombre del inyector.
- *Ruta de acceso del programa:* examine para seleccionar el programa.

- *Nodo Filtro web panel > Configuración*

El filtro web bloquea ciertos tipos de información para que no aparezcan en el navegador. Este panel le permite establecer la configuración predeterminada para el filtro Web.

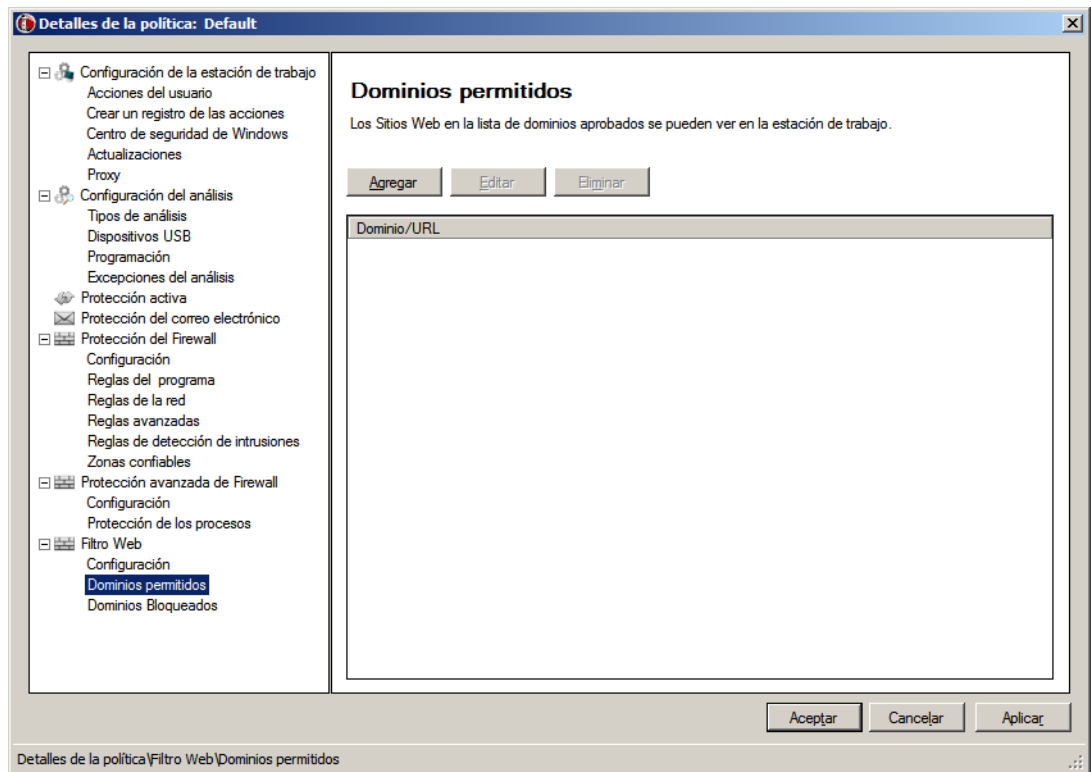


- Seleccione *Habilitar filtro web* para habilitar esta función.
- Seleccione *Registrar cuando las conexiones están bloqueadas* para garantizar que la acción realizada por Faronics Anti-Virus queda registrada en el archivo de registro.

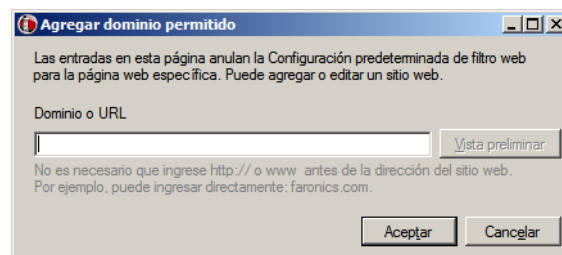
- *Nodo Filtro web panel > Dominios permitidos*



Dominios permitidos anula la configuración de filtro web predeterminada y los sitios web agregados a la lista de publicidades bloqueadas.

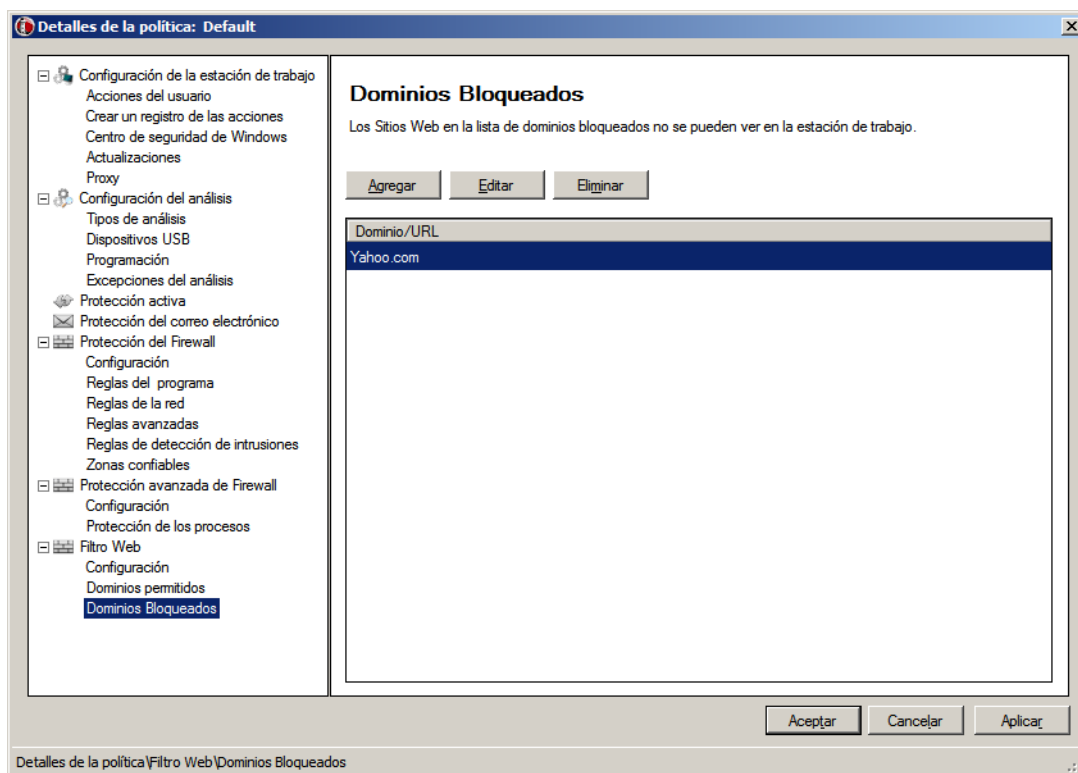


Haga clic en **Agregar** para agregar un Dominio permitido. Especifique o seleccione las opciones y haga clic en **Aceptar**. Se mostrarán los siguientes parámetros:

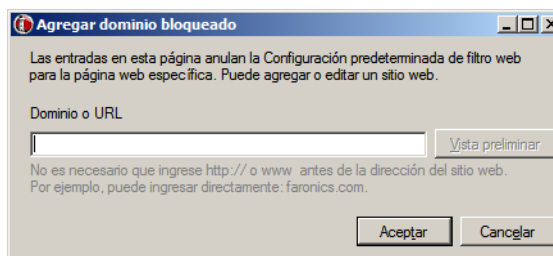


- Dominio o URL: especifique el dominio o la URL que se permitirán. Haga clic en Vista preliminar para ver una vista preliminar del dominio o la URL.
- Nodo *Filtro web* panel> *Dominios bloqueados*

Especifique los dominios que se deben bloquear en la red.



Haga clic en *Agregar* para agregar un Dominio bloqueado. Especifique o seleccione las opciones y haga clic en *Aceptar*. Se mostrarán los siguientes parámetros:



- Dominio o URL: especifique el dominio o la URL que se permitirán. Haga clic en Vista preliminar para ver una vista preliminar del dominio o la URL.
12. Haga clic en *Aceptar*. La política nueva *Política nueva 1* se muestra debajo del nodo *Anti-Virus*.

Aplicación de una política Anti-Virus

Una vez que la política Anti-Virus se ha creado, se puede aplicar a una o más estaciones de trabajo a través de Faronics Core Console. Realice los siguientes pasos para aplicar la política:

1. Seleccione una o más estaciones de trabajo. Haga clic con el botón derecho del mouse y seleccione *Reasignar política*.



2. Aparecerá el diálogo *Reasignar estaciones de trabajo a la política*. Seleccione la política del menú desplegable *Asignar política* y haga clic en *OK (Aceptar)*.
3. La política se aplica a las estaciones de trabajo seleccionadas.

Visualización o modificación de una política Anti-Virus

Una vez que la política Anti-Virus fue creada, se puede ver o modificar. Realice los siguientes pasos para ver o modificar una política:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Nombre de Core Server]>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus>[Nombre de la política]*.
3. Haga clic derecho en la política y seleccione *Detalles de la política*.
4. Para editar la política, modifique la configuración en las fichas como se explica en [Creación de políticas Anti-Virus](#).
5. Haga clic en *OK (Aceptar)* para aplicar los cambios.
6. Los cambios realizados a una política se aplicarán automáticamente a las estaciones de trabajo administradas por la política.

Renombrar una política Anti-Virus

Una vez que la política Anti-Virus fue creada, se le puede cambiar el nombre. Realice los siguientes pasos para cambiar el nombre de una política:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Nombre de Core Server]>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus>[Nombre de la política]*.
3. Haga clic derecho en la política y seleccione *Cambiar el nombre de la política*. Se mostrará el cuadro de diálogo *Cambiar el nombre de la política*.
4. Ingrese el *Nombre nuevo de la política* y haga clic en *OK (Aceptar)*.

Copiar una política

Una política existente se puede copiar fácilmente en una política nueva. Como alternativa, los datos de una política existente se pueden copiar en otra política existente.

Realice los siguientes pasos para copiar una política:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Nombre de Core Server]>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus>[Nombre de la política]*.
3. Haga clic derecho en la política y seleccione *Copiar política*. Se mostrará el cuadro de diálogo *Copiar política*.
4. Seleccione una *Política de destino* del menú desplegable o haga clic en *Nueva* para copiar los datos a una política nueva. Especifique un nombre para la política nueva.
5. Haga clic en *Copiar datos de la política ahora*.



Los datos se copian en una política existente o se crea una política nueva con la existente, como se seleccionó en el paso 3.

Eliminar una política Anti-Virus

Realice los siguientes pasos para eliminar una política existente:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Nombre de Core Server]>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus>[Nombre de la política]*.
3. Haga clic derecho en la política y seleccione *Eliminar política*. Se mostrará el cuadro de diálogo *Eliminar política*.
4. Haga clic en *Sí* para eliminar la política.



Si una política asignada a una estación de trabajo se elimina, se reemplazará con la política predeterminada. No es posible eliminar la política predeterminada.

Importar una política Anti-Virus

Una política Anti-Virus preconfigurada se puede importar a una política existente. Esta función ahorra tiempo ya que no es necesario volver a configurar toda la política.

Realice los siguientes pasos para importar una política existente:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Core Server]>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus>[Nombre de la política]*.
3. Haga clic derecho en la política y seleccione *Import Policy (Importar la política)*. Haga clic en *Yes (Sí)* para sobrescribir la configuración actual en la política existente.
4. Busque y seleccione la política que se importará. Sólo se pueden importar las políticas previamente exportadas a formato XML.
5. Seleccione una política exportada previamente y haga clic en *Open (Abrir)*. Se importará la política.

Exportar una política Anti-Virus

Se puede exportar una política Anti-Virus configurada previamente para volver a utilizarla. Esta función ahorra tiempo ya que no es necesario volver a configurar toda la política.

Realice los siguientes pasos para exportar una política existente:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Core Server]>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus>[Nombre de la política]*.



3. Haga clic derecho en la política y seleccione Export Policy (Exportar la política).
4. Examine para seleccionar la ubicación.
5. Especifique un nombre de archivo y haga clic en Save (Guardar). La política se exportará al formato XML.



Análisis mediante Faronics Core Console

El análisis se puede realizar en forma manual, según esté programado en la política Anti-Virus o se puede programar una tarea a través de Faronics Core Console. Realice los siguientes pasos para analizar manualmente las estaciones de trabajo a través de Faronics Core Console:

1. Inicie Faronics Core Console.
2. Vaya al panel *Lista de estaciones de trabajo*.
3. Haga clic en una o más estaciones de trabajo y seleccione *Scan (Analizar)*.
 - Seleccione *Scan (Análisis)>Quick (Rápido)* para realizar un análisis rápido.
 - Seleccione *Scan (Análisis)>Deep (Profundo)* para realizar un análisis profundo.
 - Seleccione *Scan (Analizar)>Abort (Anular)* para anular un análisis en progreso.
 - Seleccione *Scan (Analizar)>Pause (Pausar)* para pausar un análisis en progreso.
 - Seleccione *Scan (Analizar)>Resume (Reanudar)* para reanudar un análisis que esté pausado.
 - Seleccione *Fix Now (Arreglar ahora)* para descargar las últimas definiciones de virus y realizar un análisis. Si la Protección activa fue deshabilitada temporalmente por el usuario, se habilitará cuando se seleccione *Fix Now (Arreglar ahora)*.

El progreso del análisis (*% del análisis completado*) se muestra en el panel *Lista de estaciones de trabajo* en Faronics Core Console.



Si hay más de un Loadin instalado, se puede acceder al menú contextual de Faronics Anti-Virus al hacer clic derecho en una estación de trabajo, seleccionar *Faronics Anti-Virus* y luego seleccionar la acción en particular.



La protección activa debe estar habilitada para que la función *Fix Now (Arreglar ahora)* funcione a través de Faronics Core Console.



Ver y tomar medidas acerca de los archivos en cuarentena

Realice los siguientes pasos para ver los archivos que Faronics Anti-Virus puso en cuarentena:

1. Inicie Faronics Core Console.
2. Vaya al panel *Lista de estaciones de trabajo*.
3. Seleccione la estación de trabajo.
4. Haga clic derecho en la estación de trabajo y seleccione *Ver cuarentena*. Se mostrará la lista de los archivos en cuarentena.



5. Se mostrará la siguiente información acerca de cada archivo infectado:
 - Nombre de riesgo
 - Categoría de riesgo
 - Nombre del archivo
 - Ubicación original
 - Nivel de riesgo
 - Fecha en la que se agregó
 - Edad (días)
 - En cuarentena por
6. Seleccione las siguientes acciones:
 - *Detalles*: seleccione un archivo y haga clic en *Detalles* para ver los detalles del archivo infectado. Esto también muestra la acción recomendada.
 - *Seleccionar todo*: selecciona todos los archivos.



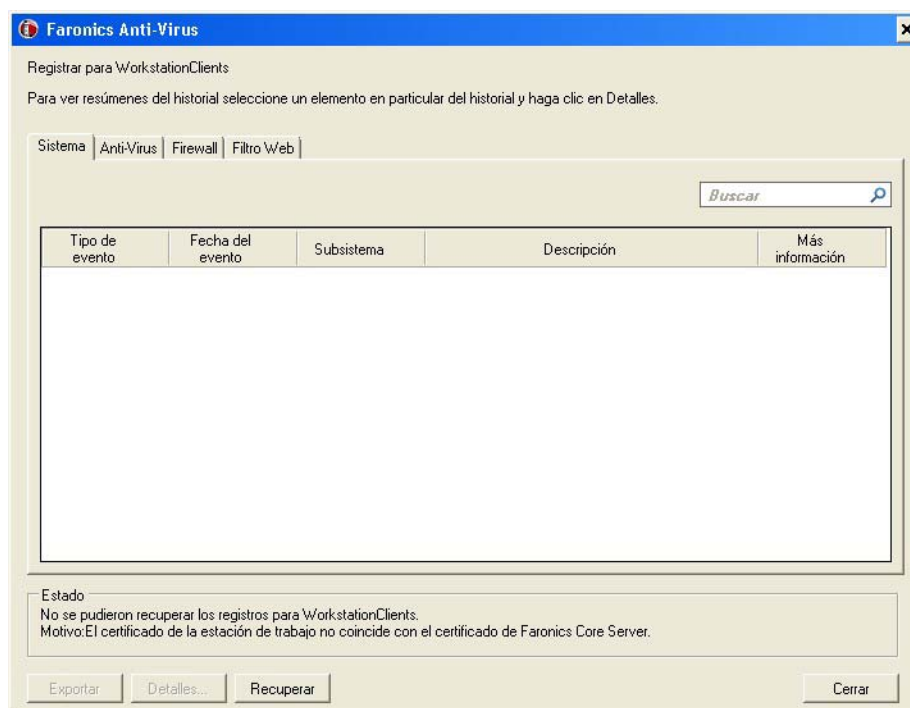
- *Eliminar del equipo*: elimina el archivo seleccionado del equipo.
- *Restaurar de la cuarentena*: restaura el archivo seleccionado del equipo.
- *Cerrar*: cierra el diálogo.



Cómo ver los registros de Faronics Anti-Virus

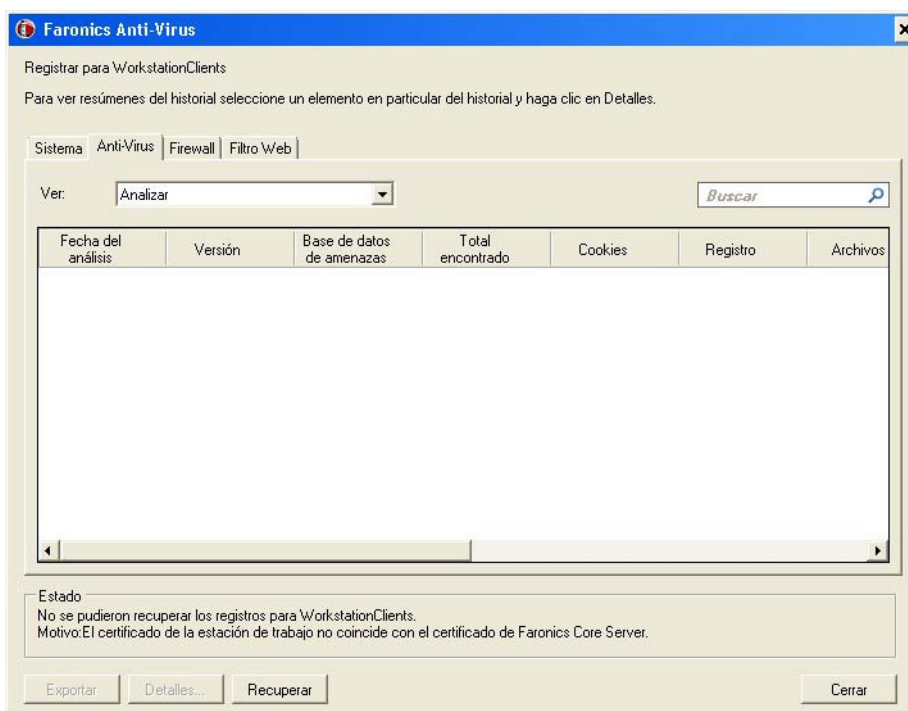
Realice los siguientes pasos para ver el registro:

1. Inicie Faronics Core Console.
 2. Vaya al panel *Lista de estaciones de trabajo*.
 3. Seleccione la estación de trabajo.
 4. Haga clic derecho en la estación de trabajo y seleccione *Ver registros*. El registro se mostrará con las siguientes fichas:
- Ficha Sistema: muestra los eventos del sistema.

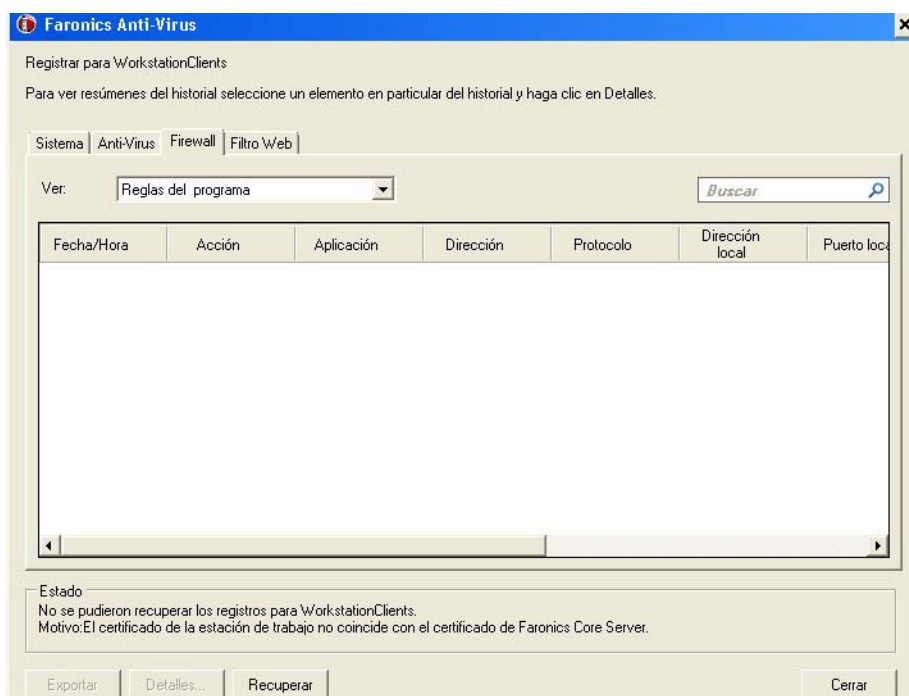




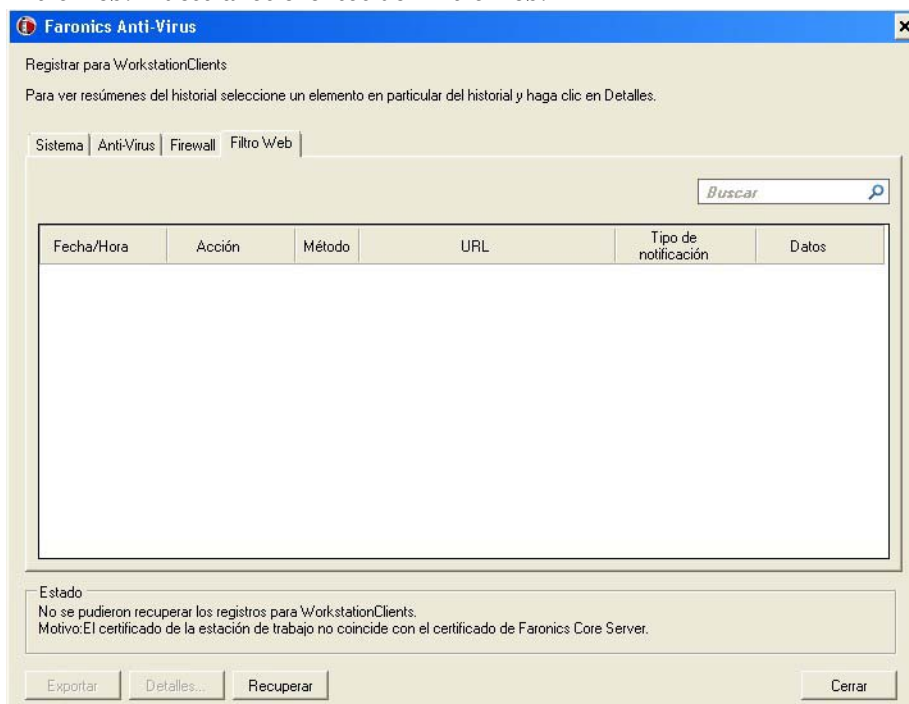
- **Ficha Anti-Virus:** muestra los eventos del Anti-Virus. Seleccione las siguientes opciones del menú desplegable para ver los resultados seleccionados para:
 - Analizar
 - Protección activa
 - Protección del correo electrónico



- **Ficha Firewall:** muestra los eventos del sistema. Busque eventos específicos en el campo Buscar. Seleccione las siguientes opciones del menú desplegable para ver los resultados seleccionados para:
 - Reglas del programa
 - Reglas de la red
 - Reglas avanzadas
 - Sistema de detección de intrusiones
 - Protección de los procesos
 - Adaptador
 - Paquetes para puertos que no están abiertos



- Ficha Filtro web: muestra los eventos del Filtro web.



5. Seleccione cualquiera de las siguientes acciones de cada ficha:
 - *Exportar*: exporta el registro a formato .txt o .csv.
 - *Detalles*: vea los detalles de la entrada del registro.
 - *Recuperar*: recupera el registro de la estación de trabajo.
 - *Cerrar*: cierra el diálogo.



Esta opción está disponible sólo cuando se selecciona una sola estación de trabajo.



Actualización de Faronics Anti-Virus a través de Faronics Core Console

Las definiciones de Faronics Anti-Virus se pueden actualizar en las estaciones de trabajo a través de Faronics Core Console. Faronics Core actúa como el depósito de actualizaciones del Anti-Virus para las estaciones de trabajo administradas. Faronics Core envía las actualizaciones del Anti-Virus automáticamente a las estaciones de trabajo remotas. Además, Faronics Core Administrator puede actualizar manualmente las definiciones de virus, como se describe a continuación.

Realice los siguientes pasos para actualizar Faronics Anti-Virus en las estaciones de trabajo:

1. Inicie Faronics Core Console.
2. Vaya al panel *Lista de estaciones de trabajo*.
3. Haga clic con el botón derecho del mouse en una o más estaciones de trabajo y seleccione *Update (Actualizar)*.
 - Seleccione *Update (Actualizar)>Full Update (Actualización total)*: esto actualiza las definiciones Anti-Virus.
 - Seleccione *Update (Actualizar)>Full Force Update (Forzar actualización completa)*: esto elimina las definiciones existentes del Anti-Virus y las actualiza con las últimas definiciones Anti-Virus.



Programación de acciones para Faronics Anti-Virus a través de Faronics Core Console

Es posible programar los eventos de Anti-Virus y de Faronics Core Console para que ocurran en una o más estaciones de trabajo en una fecha y hora convenientes para el administrador. Haga clic en una o más estaciones de trabajo y seleccione *Schedule Action (Programar acción)*. Los submenús que aparecen contienen la siguiente lista de acciones disponibles:

Acciones controladas por Faronics Core Console:

- Apagar
- Reiniciar
- Reactivar

Acciones controladas por Faronics Anti-Virus:

- Habilitar la >protección activa
- Deshabilitar >protección activa
- Análisis >rápido
- Análisis >profundo
- Actualizar>Actualización total
- Actualizar>Forzar actualización completa
- Arreglar ahora
- Instalar/Actualizar el cliente anti-virus
- Desinstalar cliente anti-virus

Al seleccionar una acción aparece un menú *Schedule (Programar)* que le permite al administrador especificar la frecuencia (una sola vez, todos los días, semanalmente, mensualmente). De acuerdo con la frecuencia, podrá seleccionar la hora, el día, la fecha o el mes.



La tarea programada a través de una política Anti-Virus siempre tiene precedencia por sobre una acción programada a través de Faronics Core Console.



Generación de informes

Faronics Anti-Virus proporciona muchos informes para monitorear la actividad de cada estación de trabajo. Hay dos categorías de informes:

- Informes globales: estos informes se basan en todas las estaciones de trabajo protegidas por Faronics Anti-Virus.
- Informes específicos de una estación de trabajo: estos informes son específicos para la estación de trabajo seleccionada.

Informes globales

Realice los siguientes pasos para generar un informe global:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console*>[Nombre de Core Server]>*Managed Workstations (Estaciones de trabajo administradas)*>*Anti-Virus*.
3. En el panel *Action (Acción)*, haga clic en *Global Reports (Informes globales)*.
4. Seleccione el informe e ingrese un rango de fechas en el diálogo que aparece. Haga clic en *OK (Aceptar)*. Estos son los informes disponibles:
 - *Amenazas por número de detecciones*: se muestran las amenazas detectadas por el número de detecciones en todas las estaciones de trabajo administradas por Faronics Anti-Virus.
 - *Resumen de gravedad de las amenazas*: se muestra el resumen de la gravedad de las amenazas.
 - *Principales 25 máquinas infectadas*: se muestran las principales 25 computadoras infectadas.
5. Se muestra el informe seleccionado en el panel *Console Tree (Árbol de la consola)* en el nodo>*Informes*.

Informes específicos de una estación de trabajo

Realice los siguientes pasos para generar un informe específico para una estación de trabajo:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console*>[Nombre de Core Server]>*Managed Workstations (Estaciones de trabajo administradas)*.
3. Seleccione la estación de trabajo para la cual desea generar el informe.
4. Haga clic derecho en la estación de trabajo y seleccione *Informes*.
5. Seleccione el informe e ingrese un rango de fechas en el diálogo que aparece. Haga clic en *OK (Aceptar)*. Estos son los informes disponibles:
 - Detalles de la estación de trabajo
 - Último análisis
 - Historial de análisis
 - Historial de protección activa
 - Cuarentena
 - Historial de protección del correo electrónico
 - Mensajes de eventos del sistema



6. Se muestra el informe seleccionado en el panel *Console Tree* (*Árbol de la consola*) en el nodo *>Informes*.

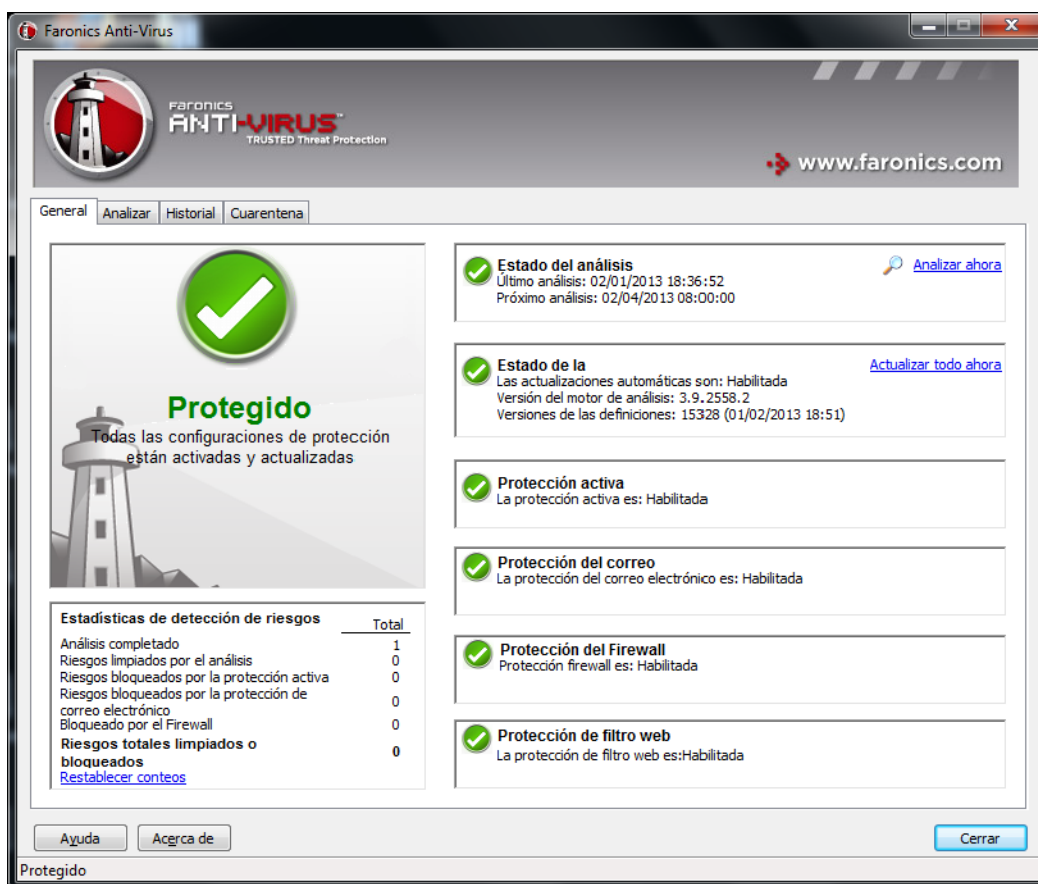


Uso de Faronics Anti-Virus en la estación de trabajo

Las funciones disponibles en Faronics Anti-Virus en la estación de trabajo dependen completamente de la configuración seleccionada en la política Anti-Virus. Para obtener más información acerca de la política Anti-Virus, consulte [Política de Faronics Anti-Virus](#).

Inicio de Faronics Anti-Virus en la estación de trabajo

Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



Los siguientes paneles muestran información importante para el usuario:

- *Protected (Protegido)* o *Not Protected (No protegido)* aparece para notificar si el equipo está protegido o no. Si aparece *Not Protected (No protegido)*, haga clic en el botón *Fix Now (Arreglar ahora)* debajo del aviso *Not Protected (No protegido)*.
- *Estado del análisis* muestra cuándo se realizó el último análisis. Para analizar ahora, haga clic en el enlace *Analizar ahora*.
- *Estado de la actualización* muestra cuándo se realizó la última actualización. Para actualizar las definiciones de virus, haga clic en el enlace *Actualizar todo ahora*.
- *Protección activa* muestra si está habilitada la protección en tiempo real.



- *Protección del correo electrónico* muestra si el correo electrónico está protegido por Faronics Anti-Virus.
- La protección del Firewall muestra si la estación de trabajo está protegida por el Firewall.
- *Protección de filtro web* aparece si la estación de trabajo está protegida por la función de Filtro web de Faronics Anti-Virus.
- *Estadísticas de detención de riesgos* muestra las estadísticas para las acciones que ha realizado Faronics Anti-Virus. Haga clic en *Restablecer conteos* para restablecer los conteos a cero.

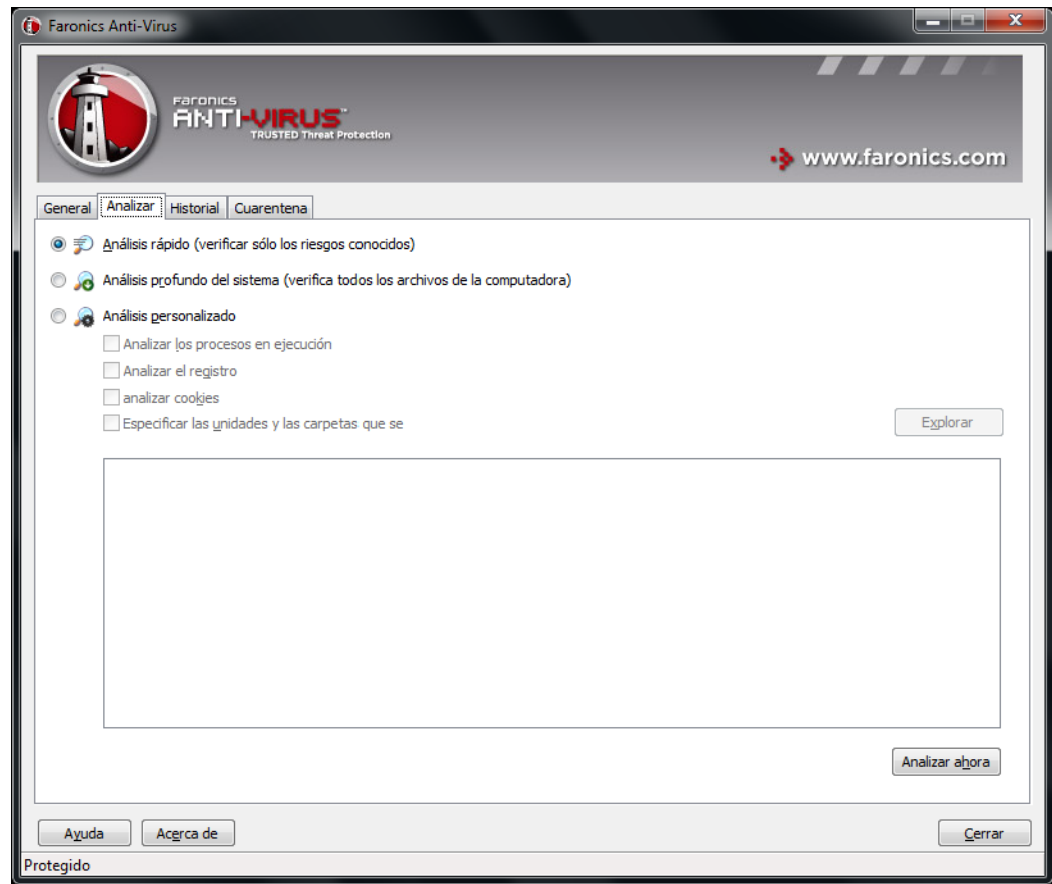
Análisis de la estación de trabajo

Realice los siguientes pasos para analizar una estación de trabajo:

1. Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



2. En el panel *Estado del análisis*, haga clic en *Analizar ahora*. Se mostrará la ficha *Analizar*. Como alternativa, también puede hacer clic en la ficha *Analizar*.



3. Seleccione una de las siguientes opciones:
 - *Análisis rápido*: analiza sólo en busca de las amenazas conocidas.
 - *Análisis profundo del sistema*: realiza un análisis detallado de todos los archivos de la estación de trabajo.
 - *Análisis personalizado* (seleccione uno de los siguientes):
 - *Analizar los procesos en ejecución*: analiza los procesos en ejecución en la estación de trabajo.
 - *Analizar el registro*: analiza el registro.
 - *Analizar cookies*: analiza los archivos cookies guardados en la estación de trabajo.
 - *Especifica las unidades y las carpetas que se analizarán*: Haga clic en *Browse (Examinar)* para seleccionar las carpetas.
4. Haga clic en *Analizar ahora*. El ícono que gira indica que se está realizando un análisis. Los resultados del análisis se muestran luego de que haya finalizado el análisis.
5. Seleccione el archivo y las siguientes opciones estarán disponibles:
 - Seleccione *Cambiar acción de limpieza*>*Acción recomendada* para realizar la acción recomendada por Faronics Anti-Virus.
 - Seleccione *Cambiar acción de limpieza*>*Poner en cuarentena/Desinfectar* para poner en cuarentena o desinfectar el archivo.
 - Seleccione *Cambiar acción de limpieza*>*Eliminar* para eliminar el archivo.
 - Seleccione *Cambiar acción de limpieza*>*Permitir* para permitir el archivo.



- Haga clic en *Seleccionar todo* para seleccionar todos los archivos que se muestran en el *Resultado del análisis*.
- Haga clic en *Detalles* para mostrar los detalles del riesgo.
- Haga clic en *Cancelar* para cerrar el diálogo sin realizar ninguna acción.
- Haga clic en *Limpiar* para eliminar el archivo y cerrar el diálogo.

La acción también se puede realizar a través de Faronics Core Console. Para obtener más información consulte [Ver y tomar medidas acerca de los archivos en cuarentena](#).

Análisis de un archivo o una carpeta con clic del botón derecho

Es muy fácil analizar en busca de virus los archivos o las carpetas (de a uno o varios). Cuando Faronics Anti-Virus está instalado en una estación de trabajo, la opción Analizar en busca de virus se agrega al menú que aparece al hacer clic derecho.

Realice los siguientes pasos para analizar un archivo o una carpeta en el equipo:

1. Haga clic con el botón derecho en el archivo o la carpeta.
2. Seleccione *Analizar en busca de virus*.

Se realizará el análisis y se mostrarán los resultados.

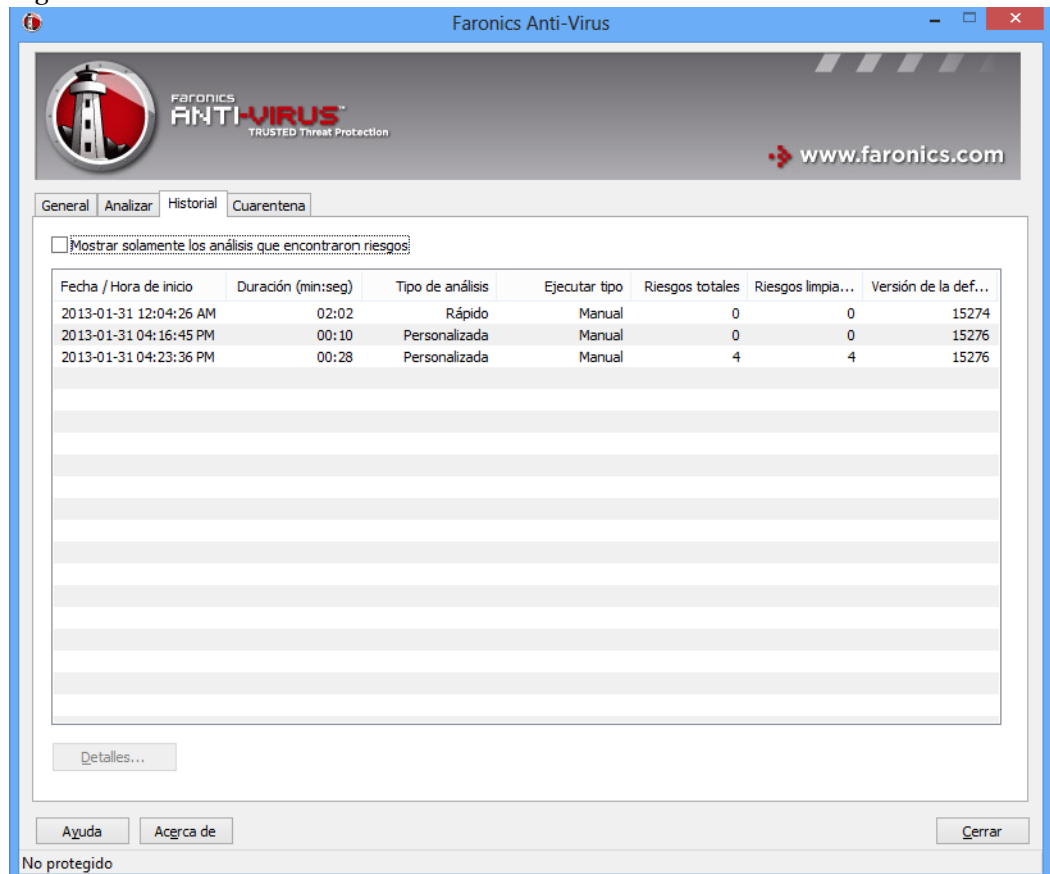
Ver historial de análisis

Realice los siguientes pasos para ver el historial de análisis:

1. Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



2. Haga clic en la ficha *Historial*.



3. Seleccione las siguientes acciones:
 - *Mostrar solamente los análisis que encontraron riesgos*: seleccione esta opción para ver solamente los análisis en los que se encontraron riesgos.
 - *Detalles*: seleccione una entrada y haga clic en los detalles para ver los detalles del análisis.

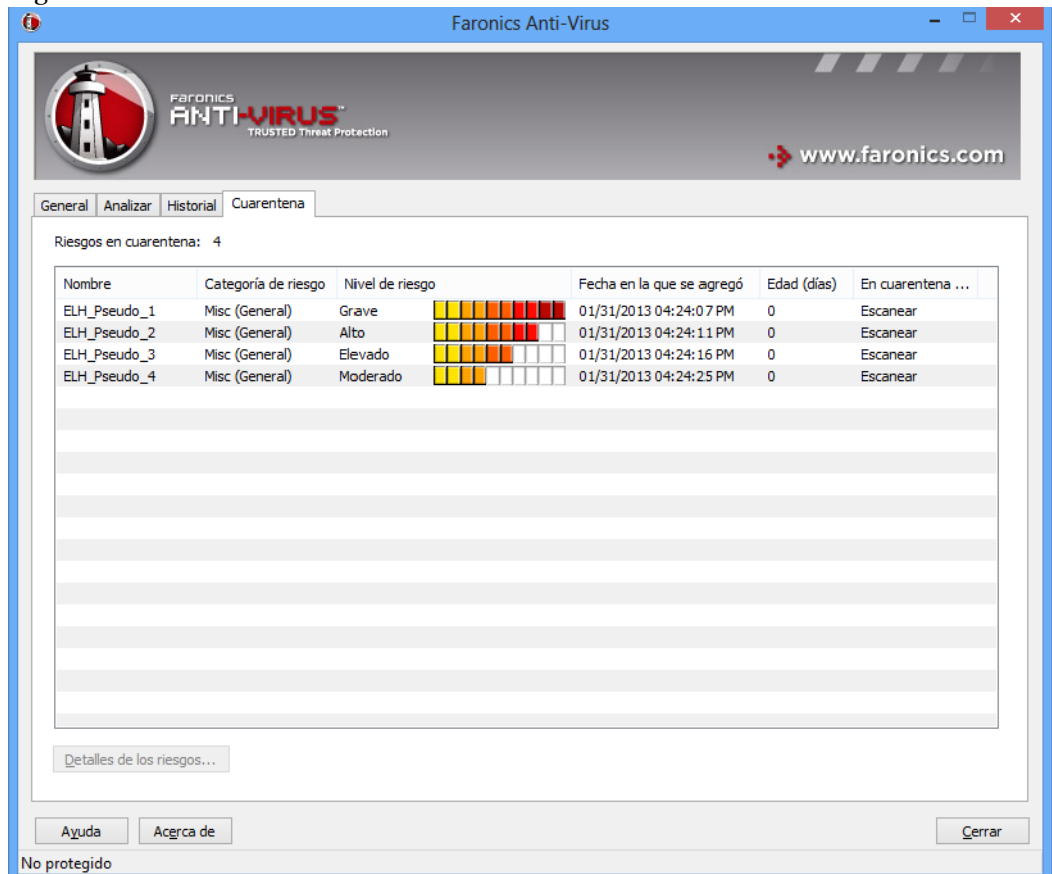
Ver y tomar medidas acerca de los archivos en cuarentena

Realice los siguientes pasos para ver Cuarentena:

1. Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



2. Haga clic en la ficha *Cuarentena*.



3. Haga clic en *Detalles de los riesgos*. Se mostrará la siguiente información acerca de cada archivo infectado:

- Nombre
- Categoría de riesgo
- Nivel de riesgo
- Fecha en la que se agregó
- Edad (días)
- En cuarentena por

4. Seleccione las siguientes acciones:

- *Detalles*: seleccione un archivo y haga clic en *Detalles* para ver los detalles del archivo infectado. Esto también muestra la acción recomendada.



Actualización de las definiciones anti-virus en la estación de trabajo

Realice los siguientes pasos para actualizar Faronics Anti-Virus en una estación de trabajo:

1. Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



2. En el panel *Estado de la actualización*, haga clic en *Actualizar todo ahora*. Se mostrará el cuadro de diálogo *Actualizar todo ahora*.
3. Haga clic en *Instalar actualizaciones*. Se actualizarán las definiciones de virus en la estación de trabajo.



Administración de Faronics Anti-Virus en la estación de trabajo a través de la bandeja de sistema

Faronics Anti-Virus se puede administrar en la estación de trabajo a través de un menú disponible en la bandeja de sistema.

Haga clic derecho en el icono de Faronics Anti-Virus en la bandeja de sistema. Estas son las opciones disponibles:

- Abrir Faronics Anti-Virus: inicia Faronics Anti-Virus en la estación de trabajo.
- *Protección activa*
 - *Protección activa>Habilitar la protección activa*: habilita la protección activa.
 - *Protección activa>Deshabilitar la protección activa>[Seleccione la opción]*: selecciona el tiempo durante el cual la protección activa estará deshabilitada. Seleccione 5 minutos, 15 minutos, 30 minutos, 1 hora, hasta que el equipo se reinicie o permanentemente. Esta opción se muestra sólo si se seleccionó en la política Anti-Virus.
- *Analizar ahora>[Seleccione la opción]*: seleccione Cancelar análisis, Pausar análisis, Reiniciar análisis, Análisis rápido o Análisis profundo. Esta opción se muestra sólo si se seleccionó en la política Anti-Virus.



Las opciones anteriores están disponibles para el usuario sólo si se especificaron en la política Anti-Virus. Para obtener más información, consulte [Creación de políticas Anti-Virus](#).



Control de línea de comandos

Este capítulo explica los diversos controles de la línea de comandos disponibles para Faronics Anti-Virus.

Temas

Control de línea de comandos



Control de línea de comandos

El control de la línea de comandos de Faronics Anti-Virus ofrece a los administradores de red una mayor flexibilidad en la administración de estaciones de trabajo con Faronics Anti-Virus al permitir el control a través de herramientas de administración de terceros y/o soluciones de administración central.

Realice los siguientes pasos para ejecutar los comandos de Faronics Anti-Virus:

1. En la estación de trabajo vaya al <directorío del sistema>: `\Program Files\Faronics\Faronics Anti-Virus Enterprise` desde la solicitud de comandos.
2. Ingrese AVECLI/ [Command]

Estos son los comandos disponibles:

Comando	Definición
definitionversion	Muestra la versión de la definición de virus.
scanengineversion	Muestra la versión del motor de análisis.
updatedefs	Actualiza y aplica las definiciones de virus.
scanquick	Inicia un análisis rápido.
scandeeep	Inicia un análisis profundo.
fixnow	Descarga la última definición de virus. Habilita la protección activa y la protección del correo electrónico. Realiza el análisis profundo predeterminado
setlicense [clave]	Aplica una clave de licencia determinada.
enableap	Habilita la protección activa.
applydefs [ruta de acceso a las definiciones]	Aplica el archivo de definiciones desde una ubicación guardada.
fixnow /quick	Realiza un análisis rápido si es

Sintaxis:

AVECLI/definitionversion



Desinstalación de Faronics Anti-Virus

Este capítulo describe cómo desinstalar Faronics Anti-Virus.

Temas

Generalidades sobre la desinstalación

Desinstalación de Faronics Anti-Virus Client a través de Faronics Core Console

Desinstalación de Faronics Anti-Virus Client de una estación de trabajo a través de Add or Remove Programs (Agregar o quitar programas)

Desinstalación de Faronics Anti-Virus Loadin con el instalador

Desinstalación de Faronics Anti-Virus a través de Agregar o Quitar Programas



Generalidades sobre la desinstalación

Faronics Anti-Virus Loadin se encuentra instalado en el sistema Faronics Core Console (o Faronics Core Server). Faronics Anti-Virus Client se encuentra instalado en las estaciones de trabajo.

Desinstale Faronics Anti-Virus Client de la estación de trabajo manualmente o a través de Faronics Core Console. Una vez que haya terminado, desinstale Faronics Anti-Virus Loadin del sistema Faronics Core Console (o Faronics Core Server).

El proceso de desinstalación se explica en las siguientes secciones.



Desinstalación de Faronics Anti-Virus Client a través de Faronics Core Console

Realice los siguientes pasos para desinstalar Faronics Anti-Virus Client a través de Faronics Core Console:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console > [Core Server] > Managed Workstations (Estaciones de trabajo administradas)*.
3. Seleccione las estaciones de trabajo de las que desea desinstalar Faronics Anti-Virus Client.
4. Haga clic con el botón derecho y seleccione *Configure Workstations (Configurar estaciones de trabajo) > Advanced (Avanzado) > Uninstall Anti-Virus Client (Desinstalar Anti-Virus Client)*.

Faronics Anti-Virus Client se desinstalará de las estaciones de trabajo.



Desinstalación de Faronics Anti-Virus Client de una estación de trabajo a través de Add or Remove Programs (Agregar o quitar programas)

Realice los siguientes pasos para desinstalar Faronics Anti-Virus a través de *Add or Remove Programs (Agregar o quitar programas)* en Windows:

1. Haga clic en *Start (Inicio)>Control Panel (Panel de control)>Add or Remove Programs (Agregar o quitar programas)*.
2. Seleccione *Faronics Anti-Virus Enterprise Workstation*.
3. Haga clic en *Remove (Quitar)*.

Faronics Anti-Virus Client se desinstalará de la estación de trabajo.



Desinstalación de Faronics Anti-Virus Loadin con el instalador

Realice los siguientes pasos para desinstalar Faronics Anti-Virus Loadin:

1. Haga doble clic en *Anti-VirusLoadinInstaller.exe*. Haga clic en *Next (Siguiente)*.

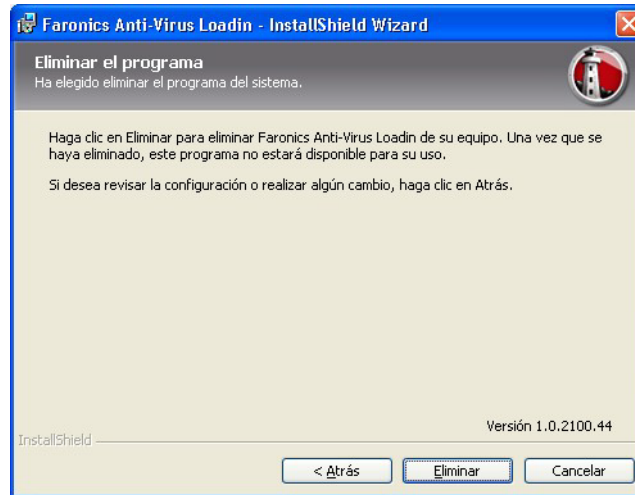


2. Seleccione *Remove (Quitar)*. Haga clic en *Next (Siguiente)*.

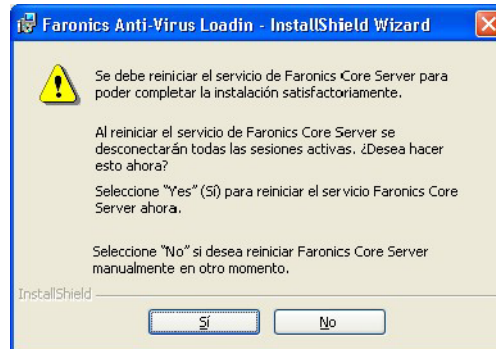




3. Haga clic en *Remove (Quitar)*.



4. Se mostrará el siguiente mensaje. Haga clic en *Yes (Sí)* para reiniciar el servicio Faronics Core Server o en *No* para reiniciar manualmente el servicio *Faronics Core Server* en otro momento.



5. Faronics Anti-Virus Loadin se quitará de su equipo. Haga clic en *Finish (Finalizar)* para completar la desinstalación.





Desinstalación de Faronics Anti-Virus a través de Agregar o Quitar Programas

Realice los siguientes pasos para desinstalar Faronics Anti-Virus Loadin a través de *Add or Remove Programs* (Agregar o quitar programas) en Windows:

1. Haga clic en *Start (Inicio)*>*Control Panel (Panel de control)*>*Add or Remove Programs* (Agregar o quitar programas).
2. Seleccione *Faronics Anti-Virus Loadin*.
3. Haga clic en *Remove (Quitar)*.

